[19]中华人民共和国专利局

[51]Int.Cl[6]
G11B 7/00
G11B 20/10 G06F 12/14
G06F 9/06

[12] 发明专利申请公开说明书

[21] 申请号 96191182.4

[43]公开日 1997 年 11 月 26 日

[11] 公开号 CN 1166223A

[22]申请日 96.10.8

[30]优先权

[32]95.10.9 [33]JP[31]261247 / 95

[32]96.1.23 [33]JP[31]8910 / 96

[32]96.8.9 [33]JP[31]211304 / 96

[86]国际申请 PCT / JP96 / 02924 96.10.8

[87]国际公布 WO97 / 14144 日 97.4.17

[85]进入国家阶段日期 97.6.6

[71]申请人 松下电器产业株式会社

地址 日本大阪

[72]发明人 大嶋光昭 后藤芳稔 田中伸一
小石健二 守屋充郎 竹村佳也

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

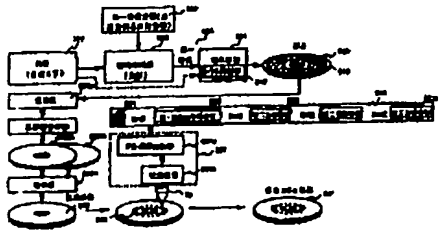
代理人 杜日新

权利要求书 6 页 说明书 22 页 附图页数 27 页

[54]发明名称 光盘,光记录装置,光重放装置,保密通信方式或程序使用许可方式

[57]摘要

为了简化利用网络型的光盘应用系统的操作程序或各种手续，在光盘设置付信息记录区域，在工厂预先记录每张光盘均不同的 ID 或密码的加密密钥或译码密钥。使用者在软件解密时通过使用 ID、密码发送时的加密密钥、密码接收时的译码密钥，可以省略程序或手续。



权 利 要 求 书

1.一种光盘，在通过微小凹凸的坑利用第一调制方式、记录主信息的光盘的第一记录区域的预定部分中，通过在半径方向部分地除去多个长形反射膜、设置利用与所述第一调制方式不同的第二调制方式、记录付信息的第二记录区域，其特征在于，在所述付信息中记录用于识别各个光盘的第一识别信息，在所述主信息之中记录利用所述第一识别信息和/或预定的通行字可以使用的不许可部分。

2.根据权利要求1的光盘，其特征在于，光盘是重放型光盘。

3.根据权利要求2的光盘，其特征在于，利用第一识别信息进行预定的运算求得预定的通行字。

4.根据权利要求1或者2的光盘，其特征在于，在付信息中，对用于识别各个光盘的第一识别信息，增加有记录密码的加密密钥和/或密码的译码密钥。

5.根据权利要求1或2的光盘，其特征在于，采用8－16调制方式作为第一调制方式，采用相位编码调制方式作为第二调制方式。

6.一种程序使用许可方式，其特征在于包括以下步骤，对于在通过微小凹凸的坑利用第一调制方式、记录主信息的光盘的第一记录区域的预定部分中，通过在半径方向部分地除去多个长形反射膜、设置利用与所述第一调制方式不同的第二调制方式、记录付信息的第二记录区域的光盘中，在所述付信息中记录用于识别各个光盘的第一识别信息和密码的加密密钥和/或密码的译码密钥，利用所述第一识别信息和/或预定的通行字，对在所述主信息中记录了成为可以使用的不许可部分的光盘进行重放；利用所述付信息重放第一识别信息，采用所述第一识别信息和/或所述预定的通行字，使所述不许可部分成为可以使用并输出。

7.根据权利要求6的程序使用许可方式，其特征在于，采用第一识别信息进行预定的运算求得预定的通行字。

8.一种保密通信方式，其特征在于包括下列步骤：对如下光盘，

在通过微小凹凸的坑利用第一调制方式、记录主信息的光盘的第一记录区域的预定部分中，通过在半径方向部分地除去多个长形反射膜、设置利用与所述第一调制方式不同的第二调制方式、记录付信息的第二记录区域，在所述付信息中记录用于识别各个光盘的第一识别信息和密码的第一加密密钥和/或密码的译码密钥，在第一计算机重放，通过所述付信息读出所述第一识别信息和所述第一加密密钥；采用所述第一加密密钥和密码算法，获得使第一数据密码化的第一密码；通过网络，把来自所述第一计算机的通信装置的所述第一密码发送至第二计算机。

9.根据权利要求8的保密通信方式，其特征在于，从主信息读出密码算法。

10.一种保密通信方式，其特征在于，包括下列步骤：在第一计算机中重放来自光盘的第一记录区域的主信息；从第二记录区域重放包含用于识别各个光盘的第一识别信息和密码的第一加密密钥和/或密码的译码密钥的付信息；通过密码算法，使用付信息中的第一加密密钥，使所述第一计算机的第一数据密码化，制作第一密码；通过网络与特定连接地址的第二计算机连接，发送所述付信息中的第一识别信息和所述第一密码；在所述第二计算机中接收所述第二识别信息和所述第一密码；从容纳了第一译码密钥和第一识别信息的对应关系的第一译码密钥数据库中，选择是与接收的所述第一识别信息对应的密码的译码密钥的第一译码密钥；根据所述第一译码密钥，对所述第一密码译码，获得所述第一数据。

11.根据权利要求10的保密通信方式，其特征在于包括下列步骤：在第一计算机中，利用生成加密密钥的第一密码生成装置，生成构成第二加密密码，以及与所述第二加密密钥成对的第二译码密钥，在所述第一计算机中，采用第一加密密钥，获得使所述第二加密密钥密码化的第三密码；向第二计算机发送所述第三密码。

12.根据权利要求11的保密通信方式，其特征在于包括下列步骤：在第二计算机中，采用第一译码密钥对接收的第三密码译码，获得第二加密密钥的普通文字；用所述第二加密密钥，获得使第二数据

密码化的第四密码；向第一计算机发送所述第四密码。

13.根据权利要求8的保密通信方式，其特征在于，从含有开放密钥系密码的付信息中重放开放密钥系密码的两个以上加密密钥和/或译码密钥的步骤中，所述加密密钥或者译码密码的密钥之中至少有一个采用椭圆函数密码。

14.根据权利要求8的保密通信方式，其特征在于，包括采用在付信息中含有第二计算机的连接地址信息的光盘，从所述付信息中重放所述连接地址的步骤。

15.一种光盘记录装置，其特征在于通过在光盘的第一记录区域的记录层上，利用光学透镜照射激光，用第一调制方式对主信息调制并记录，在记录之前，用第二调制方式，对记录了第一识别信息和密码的第一加密密钥和/或密码的译码密钥的第二记录区域的付信息进行重放，采用所述第一识别信息和/或第一加密密钥和特定的密码算法，制作使主信息密码化的主密码，在所述第一记录区域的记录层，以所述第一调制方式记录所述主密码。

16.根据权利要求15的光盘记录装置，其特征在于，由接收部接收：用第二密码算法使第一数据密码化的第二密码，和许可在光盘记录所述第一数据的记录许可信息，利用第二译码装置使所述第二密码译码的第二译码信息的获得同时，在密码运算装置中采用与所述第二密码算法不同的第一密码算法和付信息，生成使所述第二译码信息密码化的主密码，仅在所述记录许可信息存在时，在光盘的第一记录区域记录所述主密码。

17.根据权利要求16的光盘记录装置，其特征在于，安装具有运算器的IC卡，在所述IC卡输入识别付信息的盘的第一识别信息，由所述运算器对所述第一识别信息运算，用所述IC卡把运算结果输入密码运算装置，获得使第二译码信号密码化的主密码，在光盘记录所述主密码。

18.根据权利要求18的光盘重放装置，其特征在于，利用光头和第一解调装置，对在第一记录区域以第一调制方式记录了由加密装置密码化了的主密码光盘，采用第一识别信息，读出第一数据，同时

利用所述光头和第二解调装置重放在所述光盘的第二记录区域以第二调制方式记录的付信息，采用所述付信息之中的第一识别信息或者在所述第一识别信息中进行特定运算的第一付识别信息，通过译码装置对所述主密码译码，由此获得所述第一数据。

19.根据权利要求18的光盘重放装置，其特征在于，采用8－16调制解调方式作为第一解调装置的调制解调方式，采用相位编码解调方式作为第二解调装置的解调方式。

20.根据权利要求18的光盘重放装置，其特征在于，译码装置具有n个的译码密钥，根据由光盘的主信息重放的译码密钥识别信息，从所述n个之中，选择特定的1个的译码密钥。

21.根据权利要求6的程序使用许可方式，其特征在于包括以下步骤：通过网络把第一计算机连接于特定地址的第二计算机；向所述第二计算机发送用于识别付信息中的盘的第一识别信息；在所述第二计算机中，在所述第一识别信息进行特定的密码运算，把所得通行字发送至所述第一计算机；在所述第一计算机中，在译码运算部对所述通行字和所述第一识别信息进行运算，把所得第二译码码送至密码译码器；采用所述第二译码码，由所述密码译码器使所述光盘的主信息中的不许可部分成为可以使用。

22.一种对程序的非法安装的检出方式，其特征在于包括下列步骤：对在通过微小凹凸的坑利用第一调制方式、记录主信息的光盘的第一记录区域的预定部分中，通过部分地除去反射膜、设置利用与所述第一调制方式不同的第二调制方式、改写付信息的第二记录区域的光盘，在所述付信息中记录用于识别各个光盘的第一识别信息，同时第一计算机重放光盘，所述光盘在所述主信息中记录了第一程序、把所述第一程序安装在第一计算机中的硬盘的安装程序和通信程序；由所述付信息重放所述第一识别信息；把所述第一程序安装在所述硬盘中；在所述硬盘记录所述第一识别信息或者在所述第一识别信息中进行特定运算的第一付识别信息；在安装的所述第一程序的起动或者特定的操作时，所述通信程序向与所述第一计算机通过网络连接的第二计算机，发送所述第一识别信息或者所述第一付识别

信息；通过所述网络，对与所述第二计算机的硬盘中的第一识别信息对应的第二识别信息或者对第二识别信息进行特定运算的第二付识别信息进行校验；所述第一识别信息与所述第二识别信息一致时，或者所述第一付识别信息与所述第二付识别信息一致时，限制第一程序的特定操作，或者追加特定操作。

23.一种光盘，在通过微小凹凸的坑利用第一调制方式记录主信息的光盘第一记录区域的预定部分，通过在半径方向部分地除去用眼不能看出信息的条状长形反射膜，设置利用与所述第一调制方式不同的第二调制方式，以比所述主信息更低的记录密度改写付信息的第二记录区域，在所述付信息中记录用于识别各个光盘的第一识别信息，同时在所述光盘的第一记录区域的主信息中记录第一数据，作为用商品条形码用读出器读出的商品条形码，印刷与所述第一识别信息有特定对应关系的数据。

24.根据权利要求23的光盘，其特征在于，在光盘的重放面和反射侧的面上印刷商品条形码。

25.光盘中第一数据的程序使用许可方式，其特征在于包括下列步骤：对于在通过微小凹凸的坑利用第一调制方式、记录主信息的光盘的第一记录区域的预定部分中，通过部分地除去反射膜、设置利用与所述第一调制方式不同的第二调制方式、改写付信息的第二记录区域的光盘，在付信息记录用于识别各个光盘的第一识别信息的同时，在所述光盘的第一记录区域的主信息中，包含不允许使用的不许可部分，同时从印刷了用商品条形码用读出器可以读出所述第一识别信息或者与所述第一识别信息有特定关系的第一付识别信息的条形码的光盘中，在第一计算机，用所述商品条形码用读出器，读出所述第一识别信息或者所述第一付识别信息；通过网络向第二计算机发送所述第一识别信息或者所述第一付识别信息；由所述第二计算机，根据所述第一识别信息，进行密码运算，制作许可使用所述不许可部分的许可信息；向所述第一计算机发送所述许可信息；由所述第一计算机，通过印刷装置在纸张上印刷所述许可信息。

26.一种光盘，在通过微小凹凸的坑利用第一调制方式、记录主

信息的光盘的第一记录区域的预定部分中，通过在半径方向部分地除去多个长形反射膜、设置由可与所述主信息做频率分离的低频带域在所述坑上改写付信息的第二记录区域，在所述付信息中记录用于识别各个光盘的第一识别信息，采用所述第一识别信息或者/和预定的通行字，在所述主信息中记录可以使用的不许可部分。

27.根据权利要求26的光盘，其特征在于，光盘是重放型光盘。

28.根据权利要求26或者27的光盘，其特征在于采用第一识别信息，进行预定的运算求得预定的通行字。

说　　明　　书

光盘、光记录装置、光重放装置、保密通信方式和程序使用许可方式

本发明涉及光盘、光盘系统及保密通信方法。

近年来，随着国际互联网等网络和光 ROM 盘的普及，使用光 ROM 盘的网络软件流通正在兴起。而且电子商交易的研讨正在进行。

作为已有技术，使用 CD－ROM 作为载体的软件电子流通系统已实用化。这种情况下，一般是采用设定通行字，对预先在 CD－ROM 记录的密码化的软件密码进行解密的方法。但是，对于 CD－ROM，由于不能在盘上追加记录，所以不能单独地设定各盘的 ID。因此，若是单纯地使用，一条通行字可以把由同一原盘制造的所有盘的密码解密。因此，使用 CD－ROM 时，必须在 PC 机一侧的硬磁盘上制做各光盘特有的 ID，通过邮件把在中心制做的 ID 送给用户。

在使用已有的光盘和光盘系统的电子流通系统中，要求在光盘或者系统中简便地提供 ID 或加密密钥。本发明的目的是实现在使用 ROM 盘的电子流通系统中简便地提供 ID 和加密密钥。

为了解决上述课题，制造在光盘的凹坑部设置重写条形码的追记区域（以下省略记为 BCA）的光盘时，根据每张光盘 ID 必须不同的需要，在 BCA 区域分别记录通信用的加密密钥、通信用的译码密钥密码电文的译码密钥，由此在对用户分配光盘时，对用户自动地分配用户 ID 号码、通信用的发送用加密密钥、接收用的译码密钥这三者，可以省略已有系统中复杂的几个程序。这样，同时实现保密通信和存有信息的光盘的识别。

图 1 是本发明的实施例的光盘的工序图；图 2 是本发明实施例中通过脉冲激光进行微调的剖面图；图 3 是本发明的实施例的微调部的信号重放波形图；图 4 是本发明实施例的重放装置的方框图；图 5(a)是本发明的 BCA 部的重放信号波形图；图 5(b)是本发明的

BCA 部的尺寸关系图。

图 6 是本发明实施例的保密通信方法和通行字决定的加密密钥的方法图；图 7 是本发明的 BCA 的格式图；图 8 是本发明实施例的保密通信的方法和通行字决定的密码解密密钥的方法；图 9 是存储信息部分许可使用了的本发明实施例光盘的操作程序图。

图 10 是在本发明实施例的 RAM 盘记录 BCA 时的方框图；图 11 是本发明实施例的防止非法复制方式的方框图；图 12 是本发明实施例的防止非法复制的流程图；图 13 是在本发明实施例的 BCA 上印刷商品条形码的光盘的俯视图和剖面图；图 14 是本发明实施例的使用带 BCA 的 ROM 盘和 POS 终端的 POS 收款系统的方框图。

图 15 是本发明实施例的压制工厂和软件公司及销售店的密码解除流程图；图 16 是本发明实施例的使用盘 ID 等的密码数据的密码化复合化步骤的流程图(之一)；图 17 是本发明实施例的使用盘 ID 等的密码数据的密码化复合化步骤的流程图(之二)；图 18 是本发明实施例的使用 BCA 的通信加密密钥的分配和保密通信的流程图(之一)；图 19 是本发明实施例的使用 BCA 的通信加密密钥的分配和保密通信的流程图(之二)；图 20 是本发明实施例的使用 BCA 的通信加密密钥的分配和保密通信的流程图(之三)。

图 21 是本发明实施例的使用了 BCA 的电子收款系统的流程图(之一)；图 22 是本发明实施例的使用 BCA 的电子收款系统的流程图(之二)；图 23 是本发明实施例的使用 BCA 的电子收款系统的流程图(之三)；图 24 是本发明实施例的限制在使用 BCA 的一个 RAM 盘记录的记录重放方法的方框图。

根据实施例说明本发明。本文中，把使用 BCA 方式追记的区域称为 BCA 区域，把利用 BCA 记录的数据称为 BCA 数据。而且，把第一识别信息也称为 ID 或者光盘 ID。

图 1 展示了带有 BCA 的光盘的代表的工序。首先，利用开放密钥等的第一加密密钥 802，由密码编码器 803 使内容 777 密码化，如此得到的第一密码 805 通过主环装置等的 8－16 调制器 917 进行调制，利用激光把此调制信号作为凹凸的坑记录在原盘 800 的第一记

录区域919。采用此原盘800通过成型机808a成型盘状透明基片918，利用反射膜制做机808b形成Al反射膜，制做0.6毫米厚的单面盘809a、809b，利用贴合机808c完成贴合的盘809，在其第二记录区域920上，通过微调装置807，由PE调制和RZ调制组合的PE－RZ调制器807a，进行盘ID921、第一密码的译码密钥922、Internet通信用的第二加密密钥923的调制，通过脉冲激光器807b进行BCA微调，制造带有BCA的光盘801。由于使用贴合盘，所以不能改变其中包含的BCA，适合保密用途。

在说明之前，先简单的说明BCA。

如图2之(1)所示，作为BCA，利用脉冲激光808在两层盘800上，对铝反射膜809微调，根据PE调制信号记录条状纸反射部810。如图2(2)所示，在盘上形成BCA的条纹，若用通常的光头重放此条纹，由于BCA部无反射信号，所以如图2(3)所示，调制信号间断地发生欠缺的欠缺部分810a、810b、810c。调制信号由第一削波电平915进行削波。另一方面，由于欠缺部分810a等信号电平低，所以可由第二削波电平916容易地削波。如图3的记录重放波形图所示，形成的条形码923a、923b，如图3(5)所示，通过利用通常的光拾取、由第二削波电平916做电平削波，可以重放，如图3(6)所示，由LPF滤波器进行波形成形，进行PE－RZ解调，如图(7)所示，输出数字信号。结合图4说明解调操作。首先，带BCA的盘801是由两张透明基片使记录层801a位于其内部贴合而成，记录层801a有一层的情况，也有记录层801a、801b两层的情况。两层时，靠近光头6的第一层的记录层801a的控制数据中，记录表示是否记录了BCA的BCA标志922。由于在第二层801b记录BCA，首先在第一记录层801a上聚焦，并把光头6移向位于第二记录区域919的最内周的控制数据924的半径位置。由于控制数据是主信息，对其做EFM或8－15或8－16调制。仅在此控制数据之中的BCA标志922为"1"时，在1层、2层部切换部827的第二记录层801b上聚焦，重放BCA。由电平限幅器590，如图2(3)所示，一旦由一般的第一削波电平915削波，则变换成数字信号。此信号在第一解调部，由EFM925

或者8－15调制、926或者8－16调制927的解调器解调，由ECC译码器36做误差修正，输出主信息。重放此主信息中的控制数据，仅在BCA标志922为1时读出BCA。BCA标志922为1时，CPU923开始对1层、2层部切换部827发出指示，驱动焦点调节部828，从第一层的记录层801a向第二层的记录层801b转换焦点。同时，把光头6移至第二记录区域的920的半径位置，亦即在DVD标准下，在控制数据的内周侧从22.3mm至23.5mm之间记录的BCA处，读出BCA。在BCA区域，重放图2(3)所示包络线部分地欠缺的信号。在第二电平限幅器929中，设定光量比第一削波电平915低的第二削波电平916，由此可检出BCA的反射部欠缺部位，输出数字信号。在第二解调部930中对此信号做PE－RZ解调，通过在ECC译码器930d中做ECC译码，输出作为付信息的BCA数据。如此一般，由8－16调制的第一解调器928解调重放主信息，由PE－RZ调制的第二解调部930解调重放付信息即BCA数据。

图5(a)展示了滤波器943的通过前部的重放波形，(b)展示了低反射部810的槽的加工尺寸精度。槽宽在5～15μm以下是困难的。而且，如果不是在从23.5mm起的内周记录，则会破坏记录数据。因此，DVD的情形限制为最短的记录周期＝30μm、最大半径＝23.5mm，故格式化后的最大容量限制在188字节以下。

采用8－16调制方式由坑记录调制信号，获得图5(a)高频信号部933那样的高频信号。另一方面，BCA信号成为低频信号部932那样的低频信号。这样，在DVD标准的情形，由于主信息是最高约为4.5MHz的高频信号932，如图5(a)所示，付信息是周期为8.92μS即100KHz的低频信号933，所以利用LPF943可容易地对付信息做频率分离。用图4所示的含有LPF943的频率分离方式934，可将两个信号的容易地分离。这时，LPF943具有结构简单的效果。

以上是BCA的概述。

这里，利用图6通过通行字发行、保密通信和订货人的认证的操作，简要说明密码软件解密系统的全体系统。首先，对于压制工厂的工序，由于是按与图1情形基本相同的顺序制造，所以省略了原盘

800 和完成的盘 809 的图。

在压制工厂 811，对于第 1～n 号的内容的普通文字 810，通过密码编码器 812，由各个第 1～n 号的加密密钥 813，做数据的密码化或者图象信号的编码，记录在光盘的原盘 800。由此原盘 800，通过压制在制造的盘状基片 809 上形成反射膜后，把两张盘状基片贴合，作成完成盘 809。在此完成盘 809 上，在 BCA 区域 814 记录每盘不同的 ID815 或/和第一加密密钥 816（开放密钥）或/各第二加密密钥 817（开放密钥）、第二计算机的连接地址 818，把带有如此记录的盘 801 分配给用户。

由于此盘的内容被密码化，所以重放时，必须要付款，从通行字发行中心即电子商店或者购物中心收到通行字。其程序如下。

在用户的第一计算机 909，在重放装置 819 重放带有分配的 BCA 的盘 801 时，利用含 PE－RZ 解调部的 BCA 重放部 820，重放 ID815、第一加密密钥 816、第二加密密钥 817、连接地址 818 的数据。为了收到通行字，通过通信部分 822，经 Internet 等网络 823，与作为通行字发行中心 821 的服务站的第二计算机 821a 的连接地址 818 连接，向第二计算机 821a 发送 ID。

这里，说明保密通信的程序。第二计算机 821a 收到来自用户的重放装置 819 的 ID815。这样，被称为“购物中心”或“电子商店”的通行字发行中心 821 的第二计算机即服务站 821a 具有加密密钥数据库 DB824。在此数据库中，收纳了作为与此盘特有的 ID 或者 ID 的第一加密密钥 816 对应的解码密钥的秘密密钥，亦即第一解码密钥 825 和 ID 表。因此，服务站可以在接收的 ID 的条件下检索第一解码密钥 825。这样建立了从第一计算机向第二计算机 821a 的保密通信。这时，如果第一加密密钥和第一解码密钥不是开放密钥密码，而是共同密钥密码的共同密钥，则成为相同的密钥。

使用者，在盘 801 中，例如利用收纳的 1000 条密码化的内容之一、例如内容编号 826 为 n 的内容时，内容编号 826 即 n 采用作为第一加密密钥 816 的开放密钥，在由开放密钥密码函数构成的第一密码编码器 827，把密码化的密码发送到第二计算机 821a。在第二计

算机 821a 一侧，检索为了对上述的密码解码的第一解码密钥 825。从而可使此密码确实成为普通文字化。这样，获得利用密码保守用户的订货信息的秘密的效果。

此时，也可以用作为第一加密密钥 816 的开放密钥密码的秘密密钥来签名。此方法称为“数字签名”。详细的操做说明，可以参看密码的专业书，例如“E－Mail Security by Bruce Schneier 1995”的“Digital Signature”项目等。

若返回保密通信，此密码通过通信部分 822 和网络 823，送至通行字发行中心 821 的第一密码解码器 827。这样，使用与第一加密密钥 816 相应的第一对加密密钥 825，由第一对密码解码器 827 对密码解码。

这时，由于只是特定的一张光盘具有开放密钥，所以可以排除来自第三者的盘的非法订购。亦即，由于可以认证一张盘，所以可以认证此盘的持有人的用户个人。这样，由于证明了此内容编号 n 是特定的个人的订购，所以排除了第三者的非法订购。

如果此时把开放密钥 816 预先设成秘密的，可以利用此手段作为信用卡号等高度保密要求的帐号信息的发送上的技术应用。但是，在通常称为“购物中心”的商店，由于无保密的保证，不用电子付款来处理用户的帐号信息。只有信用卡系统和银行系统的帐户中心 828，才能办理用户的金融信息。目前，SET 等保密标准的统一化得以开发，使用 RSA1024bit 的开放密钥密码，实现金融信息的密码化的可能性较高。

以下，展示本发明情况的帐户信息的保密通信程序。首先，在 BCA 重放部 820 使用重放的开放密钥密码的第二加密密钥 817，使用第二密码编码器 831，通过 RSA 等的开放密钥系统密码，对个人信用卡编号等帐户信息 830 做密码化处理，由通信部 822 通过第二计算机 821 送至第三计算机 828 的密码译码器 832。在此时的数字式签名的情况下，第二加密密 817 使用秘密钥 829。

与通行字发行中心 821 的第二计算机 821a 的加密密钥的情况程序同样地，从加密密钥数据库 DB824a 中，检索与 ID 或第二加密

密钥817对应的第二译码密钥829，用此方法，可以把第二密码译码器832中的密码化的帐户信息译码。

如果在第二密码编码器831用秘密钥，829做数字式签名，则能由第二密码译码器832确认用户的签名。这样，帐户中心828使用Internet也能安全地得到用户的信用卡号或银行卡号或银行通行字等帐户信息。虽然Internet这样的开放网络存在保密问题，但在这样的系统，由于在BCA记录保密通信用的加密密钥(开放密钥)或者数字式签名的秘密钥，所以确实可进行保密通信或者认证。因此，具有防范由非法的第三者所做的非法付帐和非法订购的效果。而且由于能使用每张盘即每个用户不同的开放密钥，所以提高了通信的秘密性，减少了向第三者泄漏用户的账户信息的可能性。

这里，回到图6，说明通行字的发行程序和利用通行字解密的程序。在通行字发行中心821，根据ID、用户希望解密密钥的内容编号和表示用户的使用许可期间的时间信息这三种信息，通过采用开放密钥密码等的运算式的通行字生成部834，生成通行字，向第一计算机909发送。若说明最简单的构成例，由第二计算机，用开放密钥密码的开放密钥，使解除第n号内容的密码的译码密钥盘ID和混合时间信息的信息密码化，在通行字生成部834对此解密，生成混合了秘密钥的第n号通行字834a，发送到第一计算机909。第一计算机接收上述第n号通行字，用秘密钥对盘ID和时间信息和第n号内容的复合密钥译码。这里，通行字运算部836对由盘重放的BCA的ID835a、目前的第二时间信息835b、许可的ID833a和第一时间信息833做对比是否一致的运算。如果一致，则许可，向密码译码器837输出第n号译码密钥，第n号内容的密码837a被译码，输出第n号的内容838。输出期间被限制在仅为第一时间信息833与第二时间信息835b一致的期间。在第一计算机909一侧，由通行字运算部836对ID、通行字835和来自表示目前时间的时钟836b的时间信息这三种信息进行运算，如果ID和时间信息正确，由于作为运算结果输出正确的译码密钥，所以由密码译码器837对第n号密码译码，或者解除倒频，输出第n号内容838的普通文字数据，解除倒频的图象

信号或者声频信号。

这时，如果时钟836b的第二时间信息835b与通行字的第一时间信息833不一致，由于不能正确地对密码译码，所以不能重放。如果用时间信息，在租赁使用时，可以应用仅能在三日之内重放图象的时间限定型的租赁系统。

虽然结合图6用方框图说明了程序，但在以后结合图16～23说明此程序的流程。

以下说明关于加密密钥的容量的方法，这样，如图7(a)所示，通过在BCA输入第一加密密钥816和第二加密密钥817双方，可以获得保证与"购物中心"的商品交易和与"计费中心"之间的付款这两种保密的效果。

此时，关于与计费中心的保密，预定SET等的标准统一，使RSA1024亦即128字节的加密密钥容纳在第二加密密钥区域817。若这样做，由于BCA仅有188字节，在与"购物中心"的交易的加密密钥使用上仅剩有60字节。由20字节的大小，可了解作为具有与RSA1024的128字节同等程度的保密性的密码函数的椭圆函数系列开放密钥密码。

本发明中，第一加密密钥区域816a采用椭圆函数。椭圆函数由20字节得到与RSA1024同等的保密性。因此，通过使用椭圆函数，具有把第一加密密钥816和第二加密密717双方均容纳于188字节的BCA区域的效果。

如上所述，由于在光ROM盘适用BCA，所以能记录盘固有的ID编号、第一和第二加密密钥、连接的地址。在这种情况利用Internet时，自动地与购物中心连接，通过仅分配在BCA记录了加密密钥的光盘，实现了由解除内容的密码而引起的商品流通、商品购入认证和秘密保持、付款时的认证和机密性的保持等的保密性。因此，利用本发明的保密通信方法，由于向用户分配已有的ID或加密密钥，在不丧失保密性的条件下，可以省略采用IC卡、软盘或信函这些操作，具有合理化的较大效果。而且不固定作为Internet的连接地址的URL，而是变更。若在原盘上记录URL，在此URL连接则较好，但

变更时要变更原盘，在时间成本上效率变差。在 BCA 预先记录变更后的 URL，如果仅在通过 BCA 重放连接地址 931 之时，通过原盘的连接地址优先连接 BCA 连接地址 931，则不用重新制作原盘，具有连接变更后的连接地址 931 的效果。

图 6 展示了在 BCA 记录了开放密钥的第一号密钥和开放密钥的第一号密钥的情形。

在图 8 中，展示了在 BCA 记录开放密钥的第一加密密钥 816 和秘密钥的第三译码密钥 817a 两者的情况和发生密码密钥、保密通信的情况这两种实施例。由于程序与图 6 相同，所以仅说明不同点。首先，在压制工厂，在 BCA 记录第一加密密钥 816 和第三译码密钥 817a。在由来自付帐中心的开放密钥密码化的密码的接收中使用第三译码密钥 817a。此时，具有提高接收保密性的效果。

首先，利用图 8 说明通过生成加密密钥的具体保密通信的例子。由于第一加密密钥 816 是开放密钥，所以必须在 BCA 记录接收用的第三译码密钥 817a。另一方面，BCA 容量不大。而且开放密钥需要处理时间。因此，在图 8 中，在第一计算机 836，由随机数发生器等的加密密钥生成部 838a 生成开放密钥的加密密钥/译码密钥的对或者共用密钥。说明共用密钥的例子。由第一加密密钥 816 和第一密码编码器 842 使共用密钥 K838 密码化，送至第二计算机 821a。在第二计算机，用主译码密钥 844，由主密码译码器 843 使此密码普通文字化，获得共用密钥 K838a。由于双方具有共用密钥 K，通过把共用密钥 K 交给第二密码编码器 842a 和第二密码译码器 847a，可以从店向用户，即从第二计算机 821a 向第一计算机 836 保密通信。通过把当然共用密钥 K 送至第二密码编码器 827a 和第二密码译码器 845a，使从用户向店、即从第一计算机 836 向第二计算机 821a 的保密通信成为可能。在 BCA 记录作为开放密钥的第一加密密钥，说明生成加密密钥的方式的效果。首先，可以仅记录第一加密密钥，省略译码密钥的记录。因而不减少 BCA 的小容量。其次由于在 BCA 记录译码密钥，所以提高了保密性。以改变共用密钥情况下的每次密钥为好。

由于运算时间短，具有处理时间少即可完成的效果。这时，加密密钥生成部838a不是共用密钥，在生成开放密钥密码的一对加密密钥和译码密钥时，向第二计算机821a密码发送加密密钥，作为第二密码编码器842a的加密密钥使用，如果作为第二密码译码器847的译码密钥使用复合密钥，与处理时间长的共用密钥相比，可以进一步提高保密性。处理CPU的性能高时，可期望使用开放密钥。新生成开放密钥时，由于在BCA仅记录第一加密密钥的开放密钥，不发生保密问题。不消耗BCA的容量。而且由于不必改变加密密钥，也容易维护。

这次，由通行字发行中心821的第二计算机821a定义共用密钥K838时，使用第三加密密钥839，由第三密码编码器840使共用密钥密码化，向PC机836发送。在PC机836一侧，使用作为由BCA重放的秘密钥的第三译码密钥837，通过由第三密码译码器841进行普通文字化，获得共用密钥K838b。此时，由于仅有用户持有是秘密钥的第三译码密钥817a，所以具有能防止从中心向用户的通信内容泄漏给第三者的效果。图7(b)展示了此时的格式。如果使用椭圆函数，由于20字节就足够了，所以能把第三译码密钥839b容纳于BCA。

接着结合图9说明在密码化盘使用BCA，削减原盘制作费的实施例。

如果是n个例如1000条普通文字的内容850，使用各第1～m号的加密密钥851，由密码编码器852实施密码化。此密码化的第1～m号内容853、第1～m号内容的译码程序854a和作为对第二密码译码的程序的第二密码译码器861a，在原盘以凹凸的坑记录后，在一张基片上成形，形成反射膜之后，把两张基片贴合，制成光盘801。此时，预先在BCA记录第二密码，用此密码由第二密码编码器860，对使每张盘不同的盘固有识别信息、换言之ID855和第n号例如第1号内容解密的通行字或译码密钥等的译码信息854密码化。这样一来，在重放装置，由BCA重放部820重放第二密码。由于是由重放BCA以外的通常的记录数据的数据重放部862来重放第二

密码译码器 861，所以用此对第二密码译码，重放 ID855a 和第 n 号的通行字 854a。在密码译码器 855b，采用由数据重放部 862 重放的第 n 号内容的译码程序 854a，使用 ID855a 和通行字 854a 对第一密码译码，获得第 n 号内容的普通文字 855c 和识别信息 855a。对于 PC 机的情况，在硬磁盘 863 记录内容的 ID。此 ID855a，由于在程序起动时对 ID 与网络上是否相同进行校验，进行网络保护，所以具有能防止软件的非法安装的附带效果。亦即，如果预先在一张原盘输入密码化的一千条内容，记录与特定软件对应的通行字等的译码信息，这实质上等价于制作特定的一条内容的光 ROM 盘。用一张原盘获得与对 1000 部软件的原盘刻槽相同的效果，具有能减少原盘制作费和时间。

图 10 中，对在 RAM 盘记录内容时使用 BCA 进行密码化的程序进行说明。首先，通过从 RAM 盘 856 到 BCA 重放部 820，对 BCA 的数据重放，输出 ID857，通过接口 858a、858b 和网络，向密码化部 859 发送。在密码化部 859，用含 ID857 的密钥在密码编码器 861 中使内容 860 密码化，或者对图象声音信号进行倒频。密码化的内容送至记录重放装置，通过记录电路 862 在 RAM 盘 856 记录。

接着，重放此信号时，通过数据重放部 865 实施主数据的解调，重放密码化的信号，在密码译码器 863 中译码。这时，从 RAM 盘 856 的 BCA 区域，通过 BCA 重放部 820，重放含有 ID857 的信息，作为密钥的一部分发送至密码译码器 863。这时，在正规的复制时，在 RAM 盘记录的加密密钥是正规的盘 ID，RAM 盘的 ID 也是正规的盘 ID，因此，进行密码的译码或者解除倒频，输出第 n 号内容的普通文字 864。在图象信息的情形，对 MPEG 信号解压缩，获得图象信号。

此时，使盘 ID 密码化作为密钥。由于在社会上仅有一个盘 ID，获得仅能复制一个 RAM 盘的效果。

这里，如果从此正规的 RAM 盘向别的 RAM 盘复制之时，若最初的正规盘 ID 为 ID1，则别的非法 RAM 盘的盘 ID 成为不同的 ID2。如果重放非法 RAM 盘的 BCA，ID2 被重放。但是，由于用

ID1 对内容密码化，所以即使对密码译码器 863 中的 ID2 解密，由于密钥不同，也不能对密码译码。这样，不能输出非法复制的 RAM 盘的信号，具有保护著作权的效果。本发明采用盘 ID 方式，具有仅能一次正规地复制的正规 RAM 盘，即使用何种驱动方式重放，也不能解密密码的效果。但是，密码化部 859 也可以由装载有密码编码器的 IC 卡来代替中心。

结合图 11 的方框图和图 12 的流程图说明防止复制的方法。在步骤 877a 执行安装程序。在步骤 877b，从贴合的光盘 801，由 BCA 重放部 820 输出付信息的 ID。在步骤 877d，从数据重放部 865，由主信息重放内容和网络校验软件 870。内容和 ID857 记录在 HDD872。在步骤 877c，对 ID857 做特定的秘密的密码运算，使其不能被非法修改，作为软件 ID 记录在 HDD857。这样，在 PC 机 876 的 HDD872 同时记录的内容和软件 ID873。这里，说明图 12 的步骤 877f 的起动程序的情况。起动程序时，在步骤 877g，重放 HDD872 的软件 ID873，通过接口 875，对网络 876 上别的 PC 机 876a 的 HDD872a 中的软件 ID873a 校验。在步骤 877h，对其它 PC 机的软件 ID873a 与本身的软件 ID873 是否为同一编号进行校验，同一编号时，向步骤 877j 前进，在画面表示是否中止 PC 机 876 的程序起动的警告信息。

在其他 PC 机的软件 ID873a 不是同一编号的情况下，至少在网络上，由于没有将内容安装于多台的迹象，可断定不存在非法复制，从而进行步骤 877k，许可程序的起动。此时通过网络，也可向其他的 PC 机发送软件 ID873。在此 PC 机上，如对各 PC 机软件 ID 的重复进行校验，能够检测出非法安装，如有非法安装，则对该 PC 机发出警告信息。

这样，在 BCA 记录 ID，在坑记录区域记录网络校验程序，由此可防止同一网络上同一 ID 的软件的多次安装。这样，实现了非法复制的简便保护。

如图 13 所示，通过涂敷由白色材料构成的可以写入的写入层 850，如此设置，不仅可以用印刷文字的笔写入通行字等，由于写入层

850 较厚，也可获得防止光盘的基片损伤的效果。作为在此写入层 850 上的 BCA 区域 801a 由微调记录的 BCA 数据 849 的一部分的盘 ID815 被做普通文字化处理，通过印刷变换为英文数字的文字 851 和一般条形码，销售店或用户用重放装置不能读出 BCA，由 POS 的条形码读出器或目视可以确认或核对。可校对的 ID 用户不必经过 PC 机把 ID 通知给中心。但是，用户用电话口头向中心传达 ID 时，通过在盘上以可目视的形式印刷与 BCA 的 ID 相同的 ID，由于用户可目视读出 ID，所以不用把盘插入 PC 机即可把 ID 传至中心。用图 13 的流程图说明光盘的制造步骤。在步骤 853d，用原盘进行盘的成形，制做坑记录的基片。在步骤 853e，制做铝反射膜。在步骤 853f，用粘接剂贴合两张盘基片，制成 DVD 盘等。在步骤 853g，在盘单面施以丝网印刷的标识印刷。此时，用条形码在原盘上记录特有的识别信息。在步骤 853h，采用 POS 用条形码的格式，利用喷墨条形码印刷机或者热复制型条形码印刷机，在每一张盘印刷不同的 ID 等识别信息。在步骤 853i，由条形码读出器读出此条形码，在步骤 853j，在盘的第二记录区域记录与识别信息对应的 BCA 数据。若按此制造方法，除 BCA 之外，包含 POS 条形码的全部工序终了后，在确认盘识别信息方面，记录 BCA 数据。如果不重放盘则不读出 BCA，但是由于密度低，用市售的条形码可读出 POS 条形码。在工厂中的所有工序中均可识别盘 ID。在 BCA 微调前，通过用 POS 条形码预先记录盘 ID，几乎可以完全防止 BCA 和 POS 条形码的误记录。

通过此 BCA 方式，说明也能二次、三次记录的 BCA 的利用方法。如图 15 所示，软件制造商可以如工序(2)所示那样，二次记录上防止盗版的标记和核对密码。在工序(2)，也可以制做记录有每一张光盘均不同的 ID 序号和与用户的秘密通信用的加密密钥的盘 944b。此盘 944c、944d 即使不输入通行字也能重放。

作为别的应用，在工序(3)，在盘 944e 记录密码化或倒频化的 MPEG 图象信号等的信息。省略对 MPEG 倒频的详细操作。软件公司制做在 BCA 二次记录了子开放密钥的盘 844f，该子开放密钥用

于在工序(4)对 ID 序号和倒频解除信息译码。此盘不能单独重放。在工序(5),销售店收取付款后,用子开放密钥和成对的子秘密钥制做通行字,在盘上三次记录。或者把印刷了通行字的收据传送给用户。在这之后,由于记录了通行字,用户可以重放盘 844g。若采用此方式,即使是未付款偷窃光盘,由于不能解除图象的倒频,所以也不能正常地重放,具有使偷窃无意义从而减少的效果。

在租赁视频软件等的店,如果永久地记录通行字,当偷窃时则可使用。此时如工序(6)所示,在店中由 POS 条形码读出器读出 BCA,在步骤 951g 发行用于倒频解除的通行字,在步骤 951i 印刷收据,在步骤 951j 交给顾客。顾客一方,在步骤 951k,于自己住宅利用十位数字键在重放机输入收据的通行字。在步骤 951p 仅在预定日期重放。在租赁时,仅给了盘的一部分软件的通行字时,欲看其它软件时,在步骤 951u 用电话通知软件的通行字,在步骤 951k 输入,由此可以重放盘的其它软件。刚才表示了租赁视频软件店的例子,然而在 PC 机软件后,销售密码化的 PC 机软件时,也可以在 POS 终端印刷并交给通行字。

利用图 14 更具体地说明图 15 的工序(5)、(6)的元件销售后,租赁店中的操作。在元件销售店接收来自制造商的密码和已进行倒频处理的盘 944f,一旦确认来自用户的付款,通过条形码记录装置 945,把盘 944f 的 ID 序号、子开放密钥的数据,经过 POS 终端 946 发送至通行字发行中心 952。对于小规模的系统,通行字发行中心,即含有子开放密钥的子秘密钥的系统也可设于 POS 终端之中。通行字发行中心在步骤 951q 输入盘 ID 序号和时间信息,在步骤 951s 进行运算,在步骤 951t,利用子秘密钥密码化,在步骤 951g,发行通行字,通过网络 948 和 POS 终端 846 把通行字发送至 BCA 条形码记录装置 945,把记录的盘 944g 交给顾客。这种盘 944g 可以原样重放。

对于租赁店或 PC 机软件店,首先在橱窗陈列未解除密码或倒频的 ROM 盘 944f。顾客指定特定的 ROM 盘 944f 时,把内置有螺旋型扫描的旋转光头 953 的圆型条形码读出器 950 压在容纳于手持

透明盒的盘 900 的中心，由此读取由盘 944f 的无反射部 915 构成的反射层的条形码，读取盘 ID 序号。通过象图 13 的 852 那样的印刷盘 ID 的商品条形码，用通常的 POS 终端的条形码读出器读取出来。也可以在原盘预先记录，从压制的圆形条形码读取。利用 POS 终端 946 处理包含这些盘 ID 的信息，在从信用卡付款的同时，如上所述，从步骤 951g 中的通行字发行中心发行与 ID 序号对应的通行字。用于租赁时，在步骤 951r 叠加限制允许视听日数用的日期信息，使盘 ID 序号密码化，制做通行字。在此通行字的情况，由于仅在特定的日期操作，所以具有可以在通行字中设定例如三日的租赁期间的功能。

这样，用于发行的解除倒频的通行字在步骤 951i 中，在收据 949 上同时印刷租出日、返回日、租赁名称费用，同时把盘交给顾客。顾客把盘 944j 和收据 949 拿回，在步骤 951k，在图 6 的第一计算机 909 的十位数字键输入部 954 输入通行字，由此，通行字 835 与 ID 序号 835a 运算，输入密码译码器 837，用译码密钥形成普通文字。仅在通行字正确时，由密码译码器 837 使程序数据解除倒频，输出图象。

此时，条形码中含有时间信息，与时钟部 836b 的日期数据核对，在一致的日期期间，进行解除倒频。而且，此输入的通行字与对应的 ID 序号同时存储在存储器 755 的非易失存储器 755a 中，用户只要输入一次通行字，不用输入两次，即可解除倒频。这样，具有可以实现流通中盘的电子密钥的开闭的效果。

结合图 16 详细说明记录了软件作为密码数据的盘的软件译码方法。

步骤 865 表示向用户分配密码数据和个别 ID 的全部流程。首先，在步骤 865a，在一张原盘的 ROM 区域，记录由秘密的第一加密密钥密码化的 m 个的数据和对密码化的 m 个的数据译码用的程序。在步骤 865b，用原盘成形基片，添加反射膜的二张基片贴合，制成多张 ROM 盘。在步骤 865c，在制成盘的不能改写的付记录区域(称为 BCA)，用与 ROM 区域不同的调制方法记录密码化数据的译码所必要的译码信息(每个压制的盘不同的盘识别信息和/或密码数据的译

码密钥)。在步骤 865d,用户重放分配的盘,选择希望的密码化数据 n,开始译码处理。在步骤 865e,用用户的第一计算机重放来自 ROM 区域的密码化数据和译码程序,从付记录区域(BCA)读出译码信息。在步骤 865f,通过联机不能得到第二译码信息的情形,在图 17 的步骤 871a,在画面表示 ID 等的译码的补助信息。在步骤 871b,用户拿到与 ID 对应的通行字等第二译码,输入第一计算机。在步骤 871c,使用数据识别信息、第二译码信息和密码化数据 n,进行开放密钥系密码函数的特定运算。在步骤 871d,如果结果正确,则在步骤 871f,使第 n 号的数据成为普通文字化,用户可以对数据 n 的软件操作。

以下,结合图 18 说明采用 BCA 的 Internet 等所必需的保密通信的方法。步骤 868 是向用户分配通信程序和通信加密密钥的方法的程序。首先,在步骤 868a,在一张原盘的 ROM 区域至少记录通信程序或连接信息。在步骤 868b,用原盘成形基片,贴合两张基片,制成多张 ROM 盘。在步骤 868c,在制成的盘的不能改写的付记录区域(BCA),在压制的盘上记录各不相同的盘识别信息和密码通信用加密密钥。根据情况,用与 ROM 区域不同的调制方法记录第二计算机的连接地址和/或保密通信用译码密钥。在步骤 868d,用用户的第一计算机重放来自 ROM 区域的通信程序和密码化程序,从付记录区域读出盘识别信息和通信用加密密钥。进入图 19,在步骤 867a,BCA 区域存在连接地址时,在步骤 867b,根据 BCA 的 URL 等的连接地址与第二计算机连接,不存在连接地址时,与步骤 867c 的 ROM 区域的连接地址的计算机连接。在步骤 867d,输入发送数据,在步骤 867e,BCA 区域存在保密通信用加密密钥时,在步骤 867g,采用 BCA 区域的保密通信用加密密钥,使发送数据密码化,制作第三密码。而且,不存在时,在步骤 867f,采用 ROM 区域或者 HDD 的保密通信用的密码密钥,使数据密码化,制作第三密码。

接着在图 20,由步骤 869 说明从第二计算机 910 生成接收的密码的译码密钥的程序。首先,在步骤 869a,通信译码密钥必要时,第一计算机进入步骤 869b,校验 BCA 中是否存在通信用译码密钥,不

存在译码化密钥时，在步骤869c，采用从ROM区域重放的密码密钥/译码密钥的生成程序，由用户的键入或者随机数发生器的数据和ROM区域重放的第二密码器，重新生成一对的第二通信加密密钥/第二通信译码密钥。在步骤869d，利用在BCA记录"第二通信加密密钥和/或用户数据"的通信加密密钥和从ROM区域重放所得的密码化软件，制作密码化的第四密码。在步骤869e，把第四密码和盘识别信息和/或用户地址，发送至从盘重放所得的连接地址的第二计算机。作为第二计算机的处理，在步骤869f，接收第四密码、数据识别信息和用户地址。在步骤869g，从译码密钥数据库中选择与盘识别信息相对的通信译码密钥，用其对第四密码译码，获得第二通信加密密钥的普通文字。在步骤869h，使用第二通信加密密钥，通过Internet908把使含有用户数据一部分的服务程序数据密码化的第五密码发送至第一计算机。在步骤869i，接收第五密码(和盘识别信息)，使用上述的第二通信译码密钥和在ROM区域记录的译码函数进行译码，获得上述服务程序数据的普通文字。这样，用图20的步骤869的方式，实现第一、第二计算机之间双向保密通信。

在图21的步骤870，说明帐户信息的接收流程。在步骤870a，输入帐户信息时，向第二计算机要求帐户通信用的开放密钥密码的第三加密密钥。在步骤870b，第二计算机向和三计算机要求第三加密密钥。省略了交换的步骤，第三计算机911向第二计算机910发送ID和第三加密密钥。在步骤870c，第二计算机接收ID和第三加密密钥，在步骤870e，采用第二通信加密密钥使第三加密密钥密码化的第七密码发送至第一计算机。第一计算机在步骤870f接收第七密码，在步骤870g，采用上述第二通信译码密钥，对接收的第七密码译码，获得第三密码密钥(开放密钥函数的开放密钥)。在步骤870h，根据需要在HDD记录第三加密密钥。在下次发送时利用。在步骤870i，输入信用卡号或付款用通行字等的机密值高的账户信息时，在步骤870j，利用第三加密密钥，经由第二计算机向第三计算机发送使上述账户信息密码化的第八密码。第二计算机在步骤870k接收第八密码，向第三计算机再传送。由于第三密码的译码密

钥仅由作为金融机构的第三计算机 912 持有，所以第二计算机的电子商店不能解读。第三计算机在步骤 870m，从加密密钥数据库利用盘等的识别信息找出与第三加密密钥对应的第三译码密钥，用是开放密钥密码的秘密钥的第三译码密钥对第八密码译码，获得账户信息的普通文字。在步骤 870n，从用户的信用信息或存款余额等金融信息核对是否能回收付款，在步骤 870p，把调查结果通知第二计算机。第二计算机即电子商店在步骤 870q 判断能否回收付款，若判断为不能，在步骤 870r，不发送商品或者不送予对加密软件译码用密钥。判断能回收付款时，如图 16 所示，密钥提供系统的情形，进入步骤 870s，通过 Internet 把加密软件的译码密钥即商品发送给用户的第二计算机。第一计算机，在步骤 870t，接收加密软件的译码密钥，在步骤 870u，解除第 n 号的加密化软件的密码，在步骤 870w，获得软件的普通文字。这样，实现了内容密钥提供系统。

此图 21 的步骤 870 的方式，根据需要，要求第三计算机即金融机构发行要求账户信息这样的高保密性的第三加密密钥。也可在 BCA 预先记录。从而，具有如下效果，可在不消耗 BCA 容量的条件下，在第三加密密钥使用 RSA2048 的 256 字节更强的 RSA 系加密密钥。由于完全无需在所有的盘的 BCA 预先记录，所以第三加密密钥的发行总数较少，减少了第三加密密钥的运算所需要的 CPU 时间。而且，由于在 BCA 无第三密码，由于不公开，保密性略有提高。此时的 BCA 的任务是：如图 19，20 所示，记录由 RSA1024 等级的加密密钥决定的秘密通信盘的识别信息。若存在一张 BCA 盘，则用于实现与第二计算机的保密通信的效果好。

以下结合图 22，说明在 BCA 记录通信加密密钥和通信译码密钥两者时的保密通信的步骤 872。在步骤 872g，第一计算机 909，把用从 BCA 重放所得的通信加密密钥使用户数据密码化的第九密码，制作原盘时在 ROM 区域记录的基本识别信息和在 BCA 区域记录的盘识别信息，发送至第二计算机 910。第二计算机，在步骤 872b，接收第九密码、盘识别信息和基本识别信息。在步骤 872c，从译码密钥数据库检索与盘识别信息相对的通信译码密钥，对第九密码译

码，获得用户数据的普通文字。在步骤 872e，从加密密钥数据库选择与盘识别信息对应的第二加密密钥，用此第二密码，向第一计算机发送服务器数据和第十密码，此第十密码是用图 21 所述程序对从第三计算机接收的第三加密密钥密码化。第一计算机在步骤 872f，接收第十密码，在步骤 872g，利用在 BCA 记录的上述通信用第二译码密钥，对接收的第七密码译码，得到服务器数据和第三加密密钥（开放密钥函数的开放密钥）的普通文字。在步骤 872h，根据需要，在 HDD 记录第三加密密钥。在步骤 872j 输入帐户信息时，进入步骤 872j，利用第三加密密钥经由第二计算机向第三计算机发送使上述账户信息密码化的第十一密码。第二计算机在步骤 872m，向第三计算机再发送第十一密码。第三计算机在步骤 872m，从第三加密密钥数据库，找出与盘等的识别信息相对的第三加密密钥，对第十一密码译码，获得账户信息的普通文字。在步骤 872n，进行对用户回收付款的可能性核对，在步骤 872p，向第二计算机发送调查结果。第二计算机在步骤 872q，核对是否能回收用户的付款。判断能够回收付款时，图 16 所示的密钥提供系统的情形，进入步骤 872s，通过 Internet 向用户的第二计算机发送加密软件的译码密钥即商品。第一计算机在步骤 872t，接收加密的软件的译码密钥，在步骤 872u，解除第 n 号的密码化软件的密码，在步骤 872w 获得软件的普通文字。这样，实现了内容的密钥提供系统。

图 22 的步骤 872 的方式的效果，由于在 BCA 区域记录加密密钥和译码密钥两者，所以其特点在于不必发送从第二计算机接收上所必需的译码密钥和加密密钥。由于 BCA 的容量最大为 188 字节，所以若是开放密钥等的加密函数，由 2 个 RSA512 用 64 字节、即 128 字节可以完成记录。可以做到在 RSA512 等级的双向的密码化。若是椭圆函数，如图 7 所示，可以容内 7～8 个，所以效果更好。

结合图 23，说明在 BCA 预先记录第一加密密钥和第三加密密钥时的操作和效果。而且，图 22 的步骤 872a～872w 和图 23 的步骤 873a～873w，由于构成基本相同，所以仅说明不同的步骤。

首先，由于在 BCA 记录保守账户信息等的金融信息的保密性的

第三加密密钥，在步骤873e中的第二、第三计算机不需要生成及发送第三加密密钥。在步骤873e、873f、873g中进行收发第十二密码。而且，在步骤873j，从BCA区域读出第三加密密钥，经过第二计算机向第三计算机发送用户的账户信息。图23的方法，由于第三加密密钥的生成、收发全都不需要，所以具有程序简单的效果。

对于电子支付系统，账户中心通常存在多个同样的信用卡公司。因此，开放密钥的第三加密密钥有必要存在多个。如图7(b)所示那样，若使用RSA加密函数，则有必要成为RSA1024等级以上即128字节以上，因而在BCA的188字节中，仅能容纳1个第三加密密钥817b。但是，近年来出现的椭圆函数系加密密钥(椭圆密码)，用小容量即可获得与RSA同等的保密性。近年来，RSA函数的RSA1024已成为金融信息的保密的最低标准。若是RSA函数则必需128字节，为获得同等的保密性，若是椭圆密码，被认为20～22字节的程度即可。因此，如图7(c)所示，可以在BCA容纳多个、最大为7～8个的处理金融信息的第三密码。通过使用椭圆密码，与现实中所必需的多个金融中心相适应，实现BCA应用的电子付账系统。虽然缩小范围说明了第三密码，但即使在第一加密密钥的开放密钥使用，由于能在多个电子商店之间保持高保密性，所以与椭圆密码的效果相同。

以下结合图24更具体地说明使用图10说明的BCA的RAM盘记录重放装置。作为一个实施例，对向所谓的按观看次数计费(Pay per View)系统中的RAM盘记录的程序予以说明。首先，CATV公司等的软件公司，在节目发送器883中，采用第一加密密钥882，在第一加密器中使图象软件等内容880密码化，生成第一密码900，向各用户的CATV译码器例如译码器886发送。在译码器886一侧，若通过网络向密钥发行中心884发送特定的节目的要求，密钥发行中心884，向第一译码器886的第一译码部887发送特定的软件、特定的译码器的系统ID序号、与特定的时间限制信息903相对的倒频解除键例如第一译码信息和包含向RAM盘记录许可卡901的第一译码信息885a。第一译码部887通过系统ID888和第一译码信息885a，对第一密码900译码，在图象信号的情形，一旦解除倒频的信

号从第三密码输出部889输出防止用其它密码复制所用倒频信号，在一般的TV899，源TV信号在防止复制的条件下可以视听。这里，记录许可码901a为NO时，不能在RAM盘894记录。但是，在OK时，可以限于一张RAM盘894中记录。对此方法予以说明。

在译码器886插入IC卡902，BCA重放部895读取RAM记录器的RAM盘894的BCA，盘ID905送至IC卡902。IC卡902对盘IC905、从译码器886所得的目前时间信息904和记录许可码901a核对，在第三密码输出部889在双方向进行信号交换方式的复制的核对907，若记录许可码和复制校验为OK，IC卡902中的第二付密码器891发行加密密钥906。在第二密码器890中，第三密码被再次加密化，用特定一张盘的盘ID，使内容880加密化的第二密码被生成，送至RAM记录器892，在记录装置893中，采用8－15或8－16调制，通过第一调制部来调制，利用激光在RAM盘894的第一记录区域894a记录第二密码912。这样，RAM盘894的数据被特定的盘ID序号加密化。

接着，由通常的重放装置896对此盘重放的信号，若由8－16调制的第一解调部896a解调，则输出内容的第二密码。第二译码器897具有多个第二译码密钥898a、898b、898c。这些成为具有与各CATV局等的节目供给公司各不相同的IC卡的加密密钥对应的译码密钥。此时，译码器886或者IC卡902的译码密钥识别信息记录时在第一记录区域894a记录。重放装置读出来自第一记录区域894a的译码密钥识别信息913，利用译码密钥区别装置914，与译码密钥898a～898z之中的原本的各加密密钥对应，自动地选择第二译码密钥898a，以盘ID905a作为一个密钥，第二密码在第二译码器897中译码。也可使用输入特定的译码密钥的IC卡。图象情形下，在TV899a获得解除倒频后的正常图象。

在图24的系统中，向各用户家中的、插在译码器中的IC卡发送盘ID905，由于图象数据等被加密化，软件公司883不必个别改变向各用户分配的内容密码。因此，向卫星广播或者CATV这样大量的视听者播送按观看次数计费的倒频图象时，具有能够许可仅在一张

RAM 盘上将各用户全都进行记录的效果。

在图 24 的系统，如果在一张盘记录的同时，若欲在第二张即其它盘 ID 的 RAM 盘上做非法复制即记录时，由于 BCA 的情形使用两层盘，不能改变盘 ID，因而防止了同时向第二张盘的非法复制。其次，在其它时间段，向译码器或 IC 卡发送模拟的记录许可码 901a 或第三密码，用特定的盘 ID 使数据加密化。考虑在其它盘 ID 的 RAM 盘记录。对这些非法行为，IC 卡之中的译码器时间信息管理部 902，比较密钥发行中心 884 的时间限制信息 903、内容的时间信息的时间和译码器之中的时间信息部 904a 的当前时间，核对时间一致，成为 OK，则 IC 卡 902 许可第二密码运算器 990 的加密化。

此时，第二密码器 890 和第一译码部 887，也可采用双向对校验数据交换通信的信号交换方式的时间校验方式。对于信号交换方式的情形，含有 IC 卡的第二密码运算器 890、第一译码部 887 和第三密码部 889，做双向加密数据的确认。由此可防止在内容的发送时间不同的时间的非法复制。

这样，在各用户持有的译码器 886 中，社会上仅存在一张的特定盘 ID 的 RAM 盘 894 的仅仅一张中，记录软件公司的内容。因此，即使在哪个 RAM 盘重放机上也能重放此盘。用图 24 的方式，即使在 RAM 盘记录时，也具有保护软件公司的著作权的效果。

而且，虽然利用本文的附图说明，说明了由密码编码器进行加密化，由密码译码器进行译码化，但实际上，也可以用作为 CPU 中的系统的加密算法语言和译码算法语言。

这样，通过在光盘的 BCA 区域预先记录 ID、密码的加密密钥或译码密钥，用更简单的程序可以实现加密化的内容的密码解除。而且无需已有的登记手续即可实现通信的机密性。通过在内容中预先容纳网络校验程序，可以防止同一网络上的同一 ID 的软件的多次安装。这样具有提高保密性的各种效果。

图 1

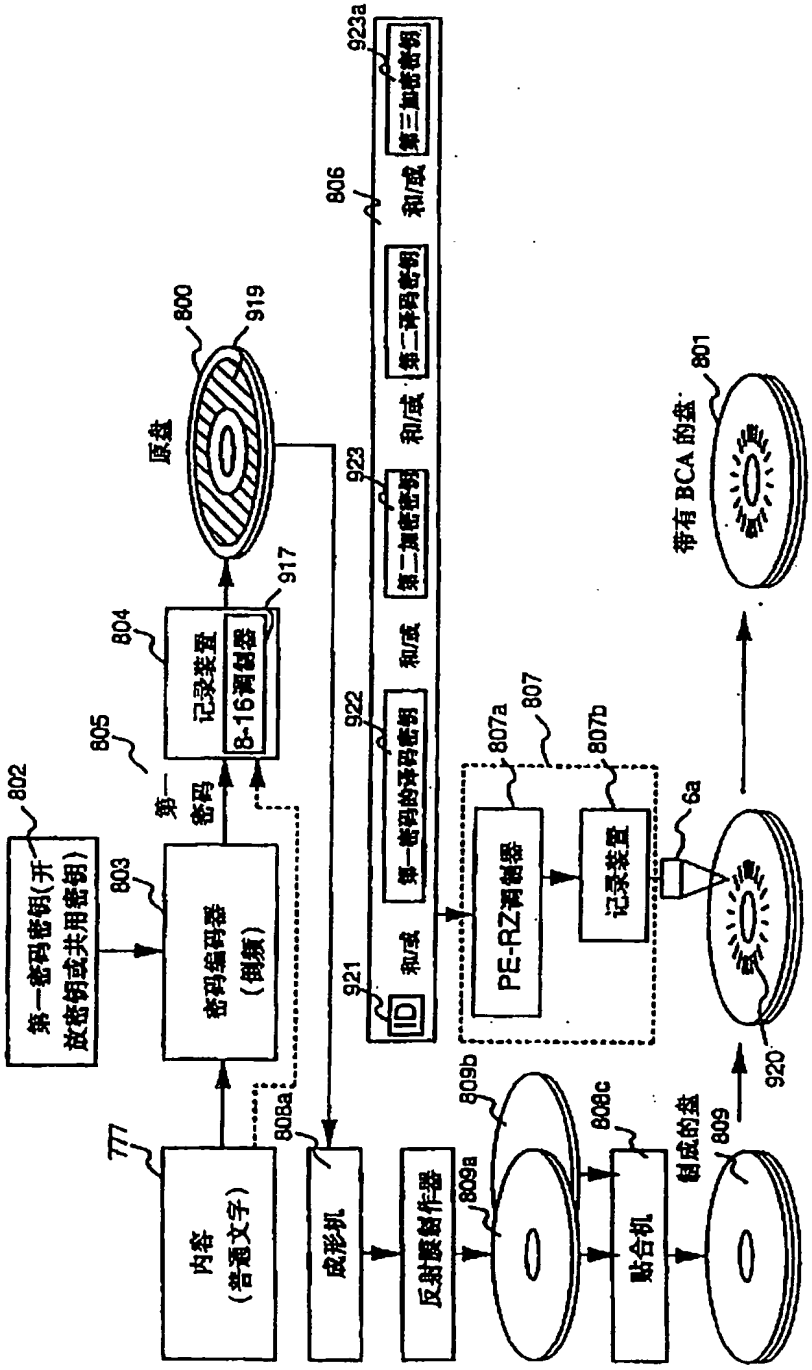

内容
(普通文字)
777
成形机
808a
反射膜制作器
809a
809b
贴合机
808c
创成的盘
809
920
带有 BCA 的盘
801
6a
PE-RZ调制器
807a
记录装置
807b
807
ID
和/成
第一密码的译码密钥
922
第一密码
密码编码器
(倒频)
803
第一密码密钥(开放密钥或共用密钥)
802
805
记录装置
8-16调制器
804
917
原盘
919
800
第二加密密钥
923
第二译码密钥
第三加密密钥
923a
806

图 2

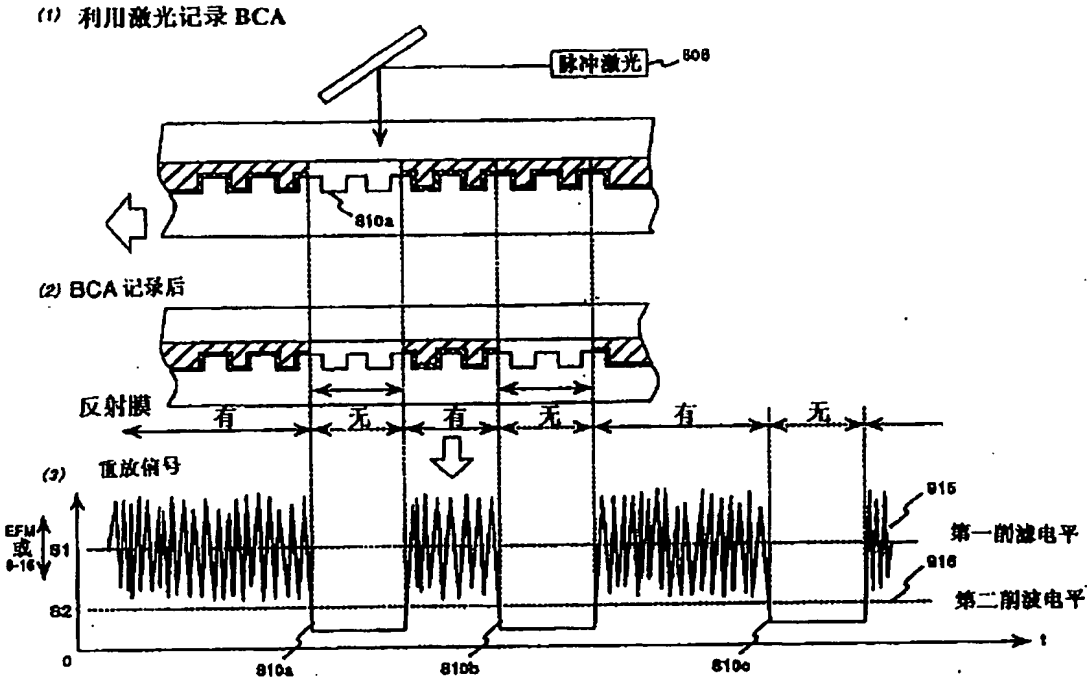

(1) 利用激光记录 BCA
脉冲激光
808
810a
(2) BCA 记录后
反射膜
有
无
有
无
有
无
(3) 重放信号
EFM
或
8-16
S1
S2
0
t
915
第一削波电平
916
第二削波电平
810a
810b
810c

图 3

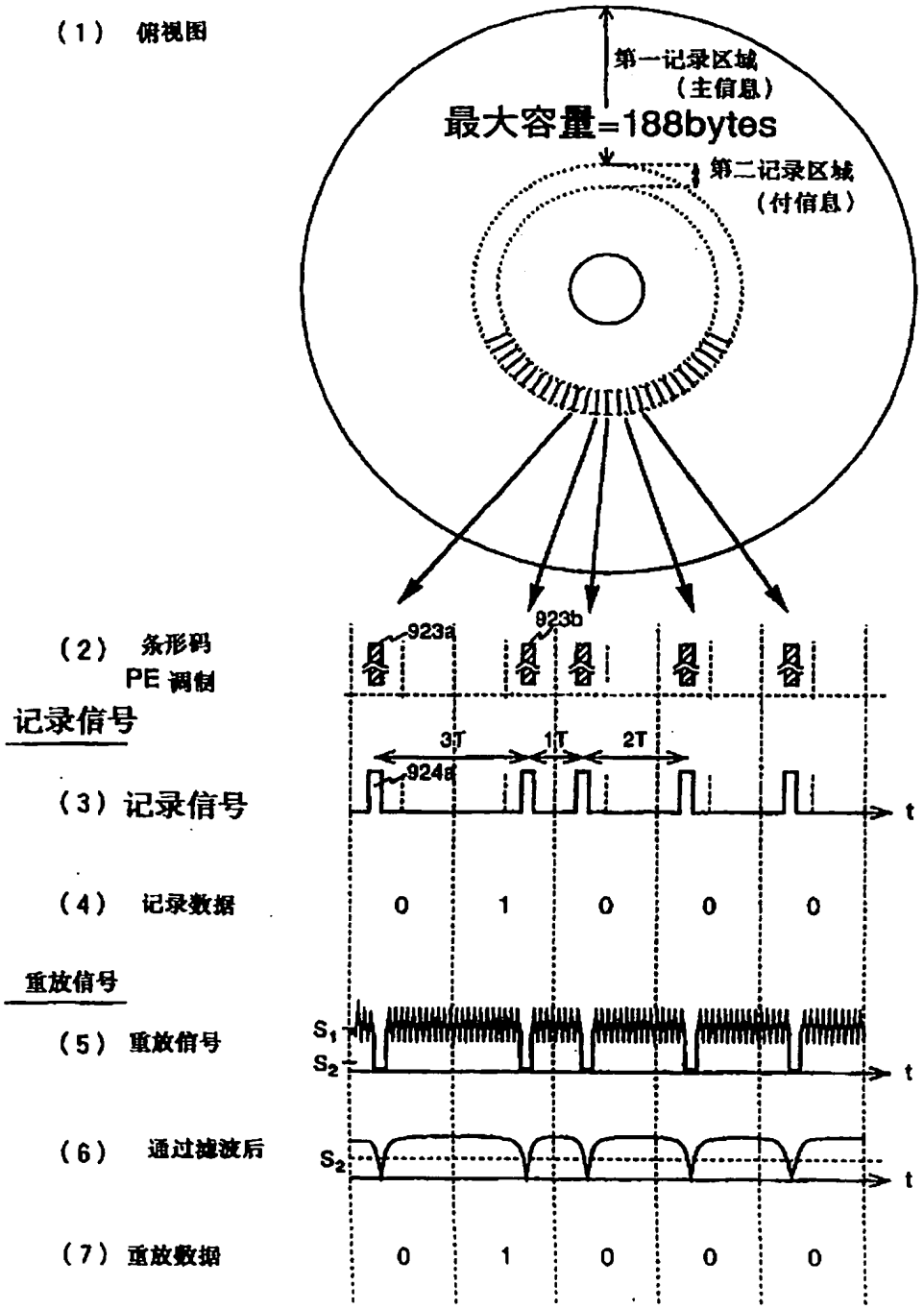
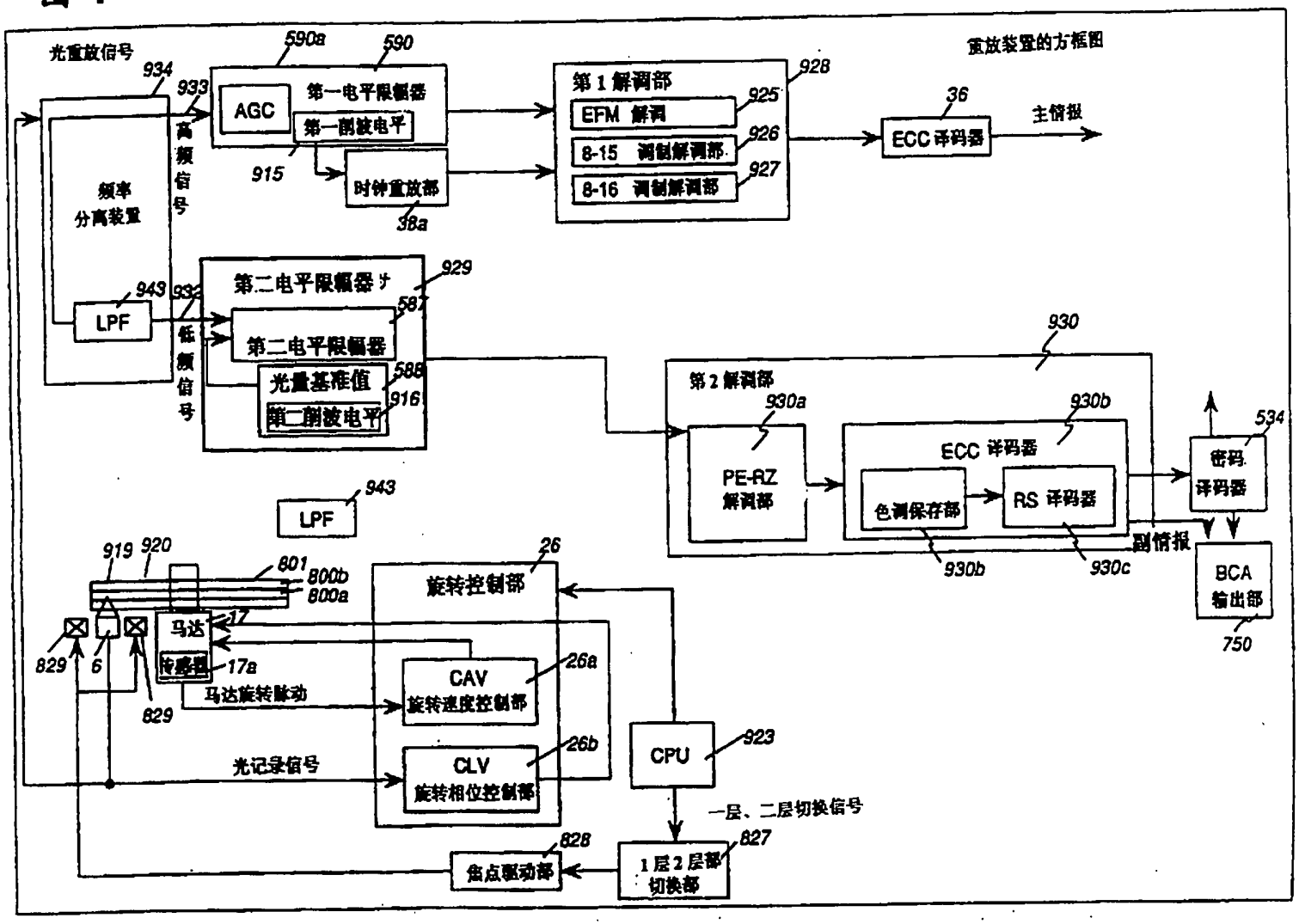

（1） 俯视图
第一记录区域
（主信息）
最大容量=188bytes
第二记录区域
（付信息）
（2） 条形码
PE 调制
923a
923b
记录信号
3T
1T
2T
924a
（3）记录信号
t
（4） 记录数据
0 1 0 0 0
重放信号
（5） 重放信号
S1
S2
t
（6） 通过滤波后
S2
t
（7）重放数据
0 1 0 0 0

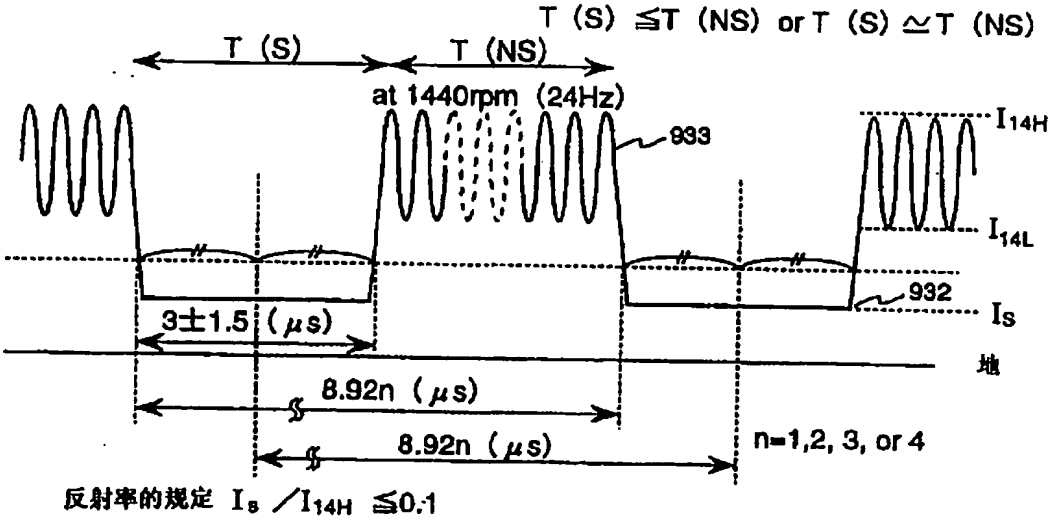
图 4


光重放信号
重放装置的方框图
934
933
590a
590
AGC
第一电平限幅器
第一削波电平
915
时钟重放部
38a
高频信号
频率分离装置
第1解调部
928
EFM 解调
925
8-15 调制解调部
926
8-16 调制解调部
927
36
ECC译码器
主情报
943
LPF
932
低频信号
第二电平限幅器
929
587
第二电平限幅器
光量基准值
588
第二削波电平
916
930
第2解调部
930a
PE-RZ 解调部
930b
ECC 译码器
色调保存部
RS 译码器
930b
930c
副情报
534
密码译码器
BCA 输出部
750
943
LPF
919
920
801
800b
800a
26
旋转控制部
829
6
马达
17
传感器
17a
829
马达旋转脉动
CAV 旋转速度控制部
26a
光记录信号
CLV 旋转相位控制部
26b
CPU
923
一层、二层切换信号
1层2层部切换部
827
焦点驱动部
828

传感器

图 5

(a) 通过滤波前的重放信号波形



反射率的规定 $I_S / I_{14H} \leqq 0.1$

(b) 槽的尺寸精度 (at r=22.2mm)

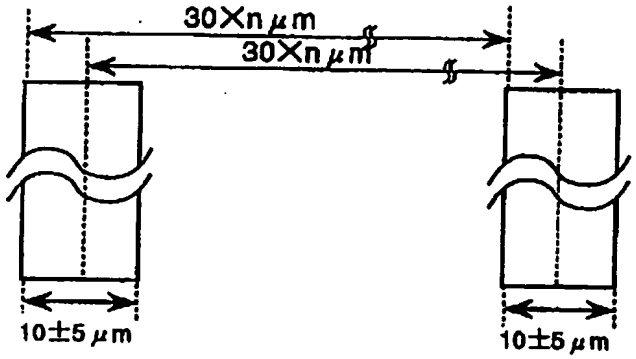


图 6

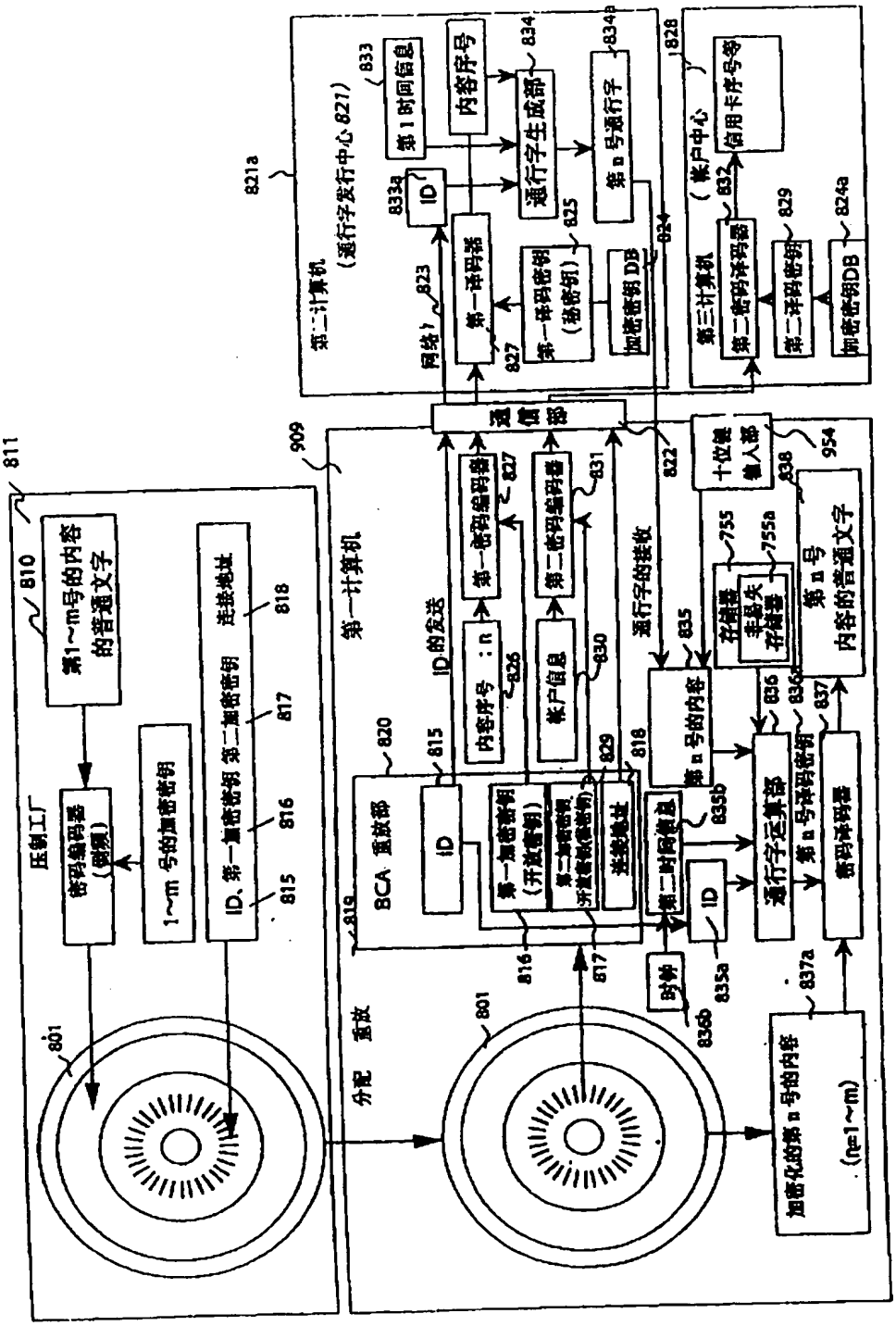

压制工厂
811
密码编码器（刻录）
第1~m号的内容的普通文字
1~m 号的加密密钥
ID、第一加密密钥 第二加密密钥 连接地址
810
801
分配 重放
第一计算机
909
BCA 重放部
820
819
ID
第一加密密钥（开放密钥）
第二加密密钥（秘密密钥）
连接地址
815
816
817
818
ID的发送
内容序号 ：n
826
帐户信息
830
第一密码编码器
827
第二密码编码器
831
通信部
822
通行字的接收
第二计时信息
829
第n号的内容
835
835b
ID
835a
时钟
836b
通行字运算部
836
第n号译码密钥
836a
密码译码器
837
837a
加密化的第n号的内容
（n=1~m）
十位键输入部
838
954
存储器
非易失存储器
755
755a
第n号内容的普通文字
第二计算机
（通行字发行中心827）
821a
网络
823
第一译码器
第一译码密钥（秘密钥）
825
加密密钥DB
824
第n号通行字
834b
通行字生成部
834
内容序号
第1时间信息
833
833a
ID
第三计算机
（帐户中心）
828
信用卡序号等
832
第二密码译码器
第二译码密钥
829
加密密钥DB
824a

图7

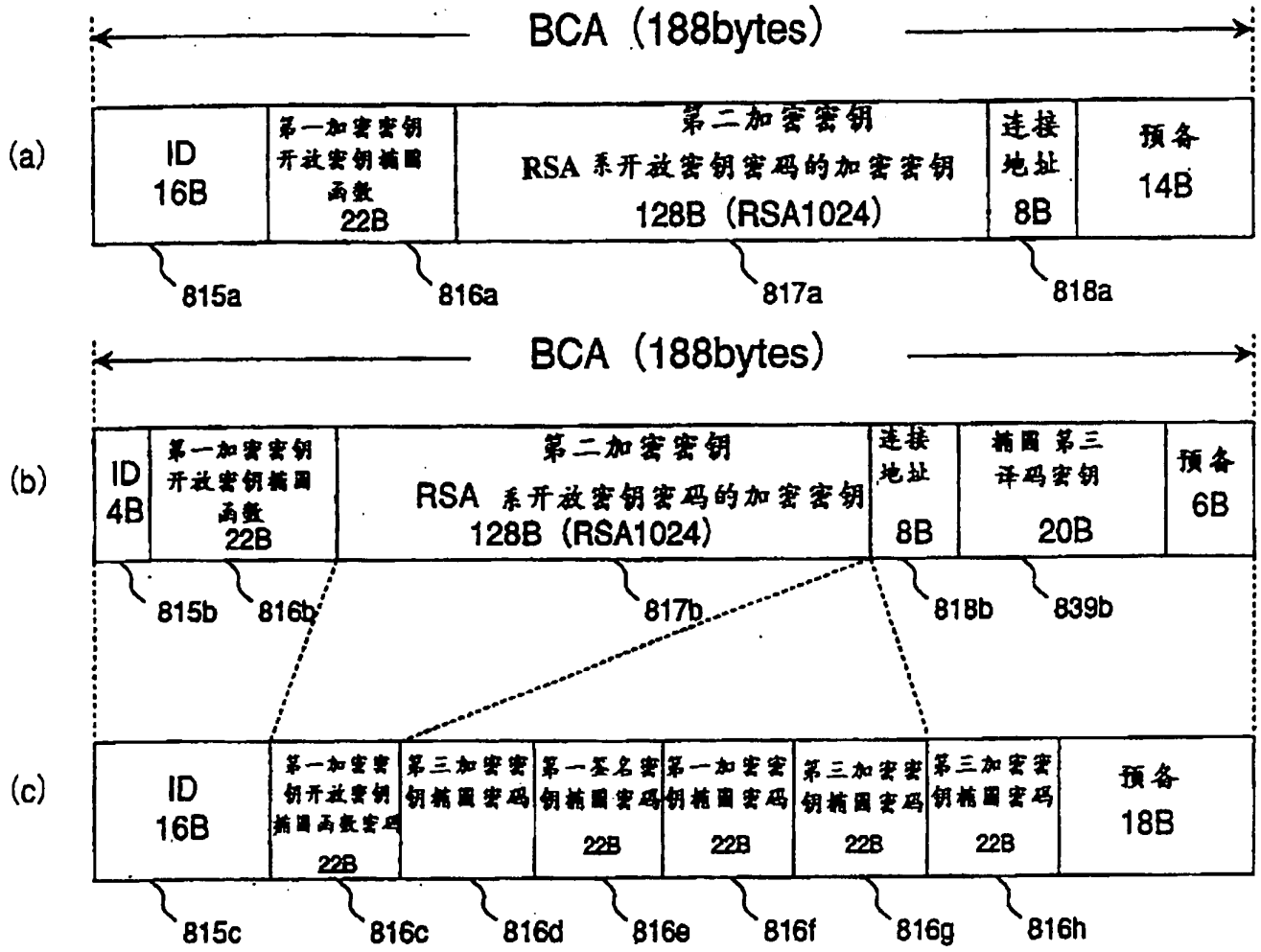

BCA (188bytes)
(a)
ID
16B
第一加密密钥
开放密钥椭圆
函数
22B
第二加密密钥
RSA 系开放密钥密码的加密密钥
128B (RSA1024)
连接
地址
8B
预备
14B
815a
816a
817a
818a
BCA (188bytes)
(b)
ID
4B
第一加密密钥
开放密钥椭圆
函数
22B
第二加密密钥
RSA 系开放密钥密码的加密密钥
128B (RSA1024)
连接
地址
8B
椭圆 第三
译码密钥
20B
预备
6B
815b
816b
817b
818b
839b
(c)
ID
16B
第一加密密钥开放密钥椭圆函数密码
22B
第三加密密钥椭圆密码
第一签名密钥椭圆密码
22B
第一加密密钥椭圆密码
22B
第三加密密钥椭圆密码
22B
第三加密密钥椭圆密码
22B
预备
18B
815c
816c
816d
816e
816f
816g
816h

图8

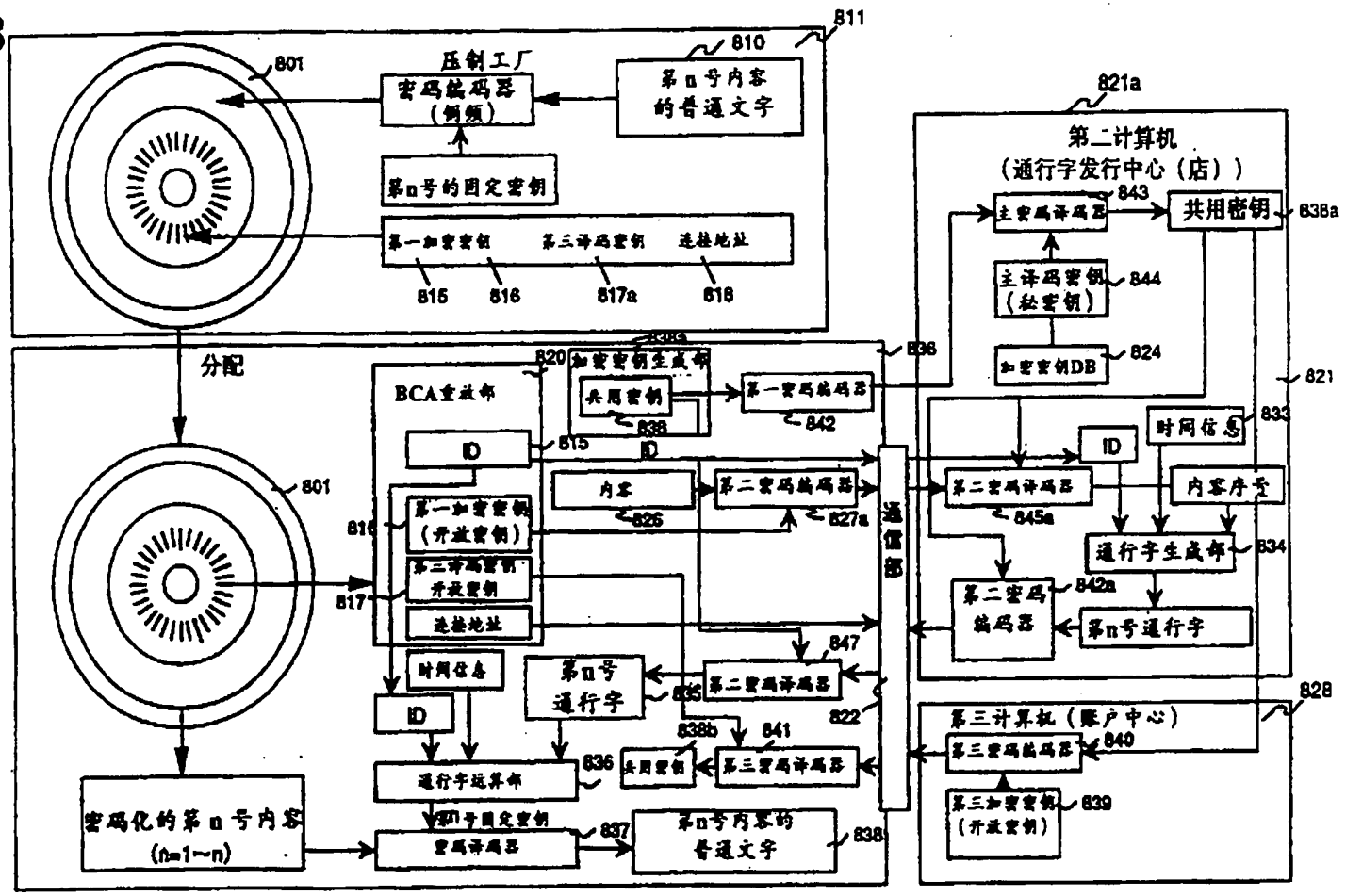

811
压制工厂
801
密码编码器（钢版）
810
第n号内容的普通文字
第n号的固定密钥
第一加密密钥
第三密码密钥
连接地址
815
816
817a
818
分配
820
BCA登录部
加密密钥生成部
838a
共用密钥
838
第一密码编码器
842
821a
第二计算机
（通行字发行中心（店））
主密码译码器
843
共用密钥
838a
主译码密钥（私密钥）
844
加密密钥DB
824
821
836
ID
815
ID
时间信息
833
内容
826
第二密码编码器
827a
第二密码译码器
845a
内容序号
第一加密密钥（开放密钥）
816
第三译码密钥开放密钥
817
连接地址
通行字生成部
834
第二密码编码器
842a
第n号通行字
847
时间信息
第n号通行字
845
第二密码译码器
822
通信部
ID
838b
841
共用密钥
第三密码译码器
通行字运算部
836
828
第三计算机（账户中心）
840
第三密码编码器
第三加密密钥（开放密钥）
839
密码化的第n号内容（n=1～n）
第n号固定密钥
密码译码器
837
第n号内容的普通文字
838

图 9

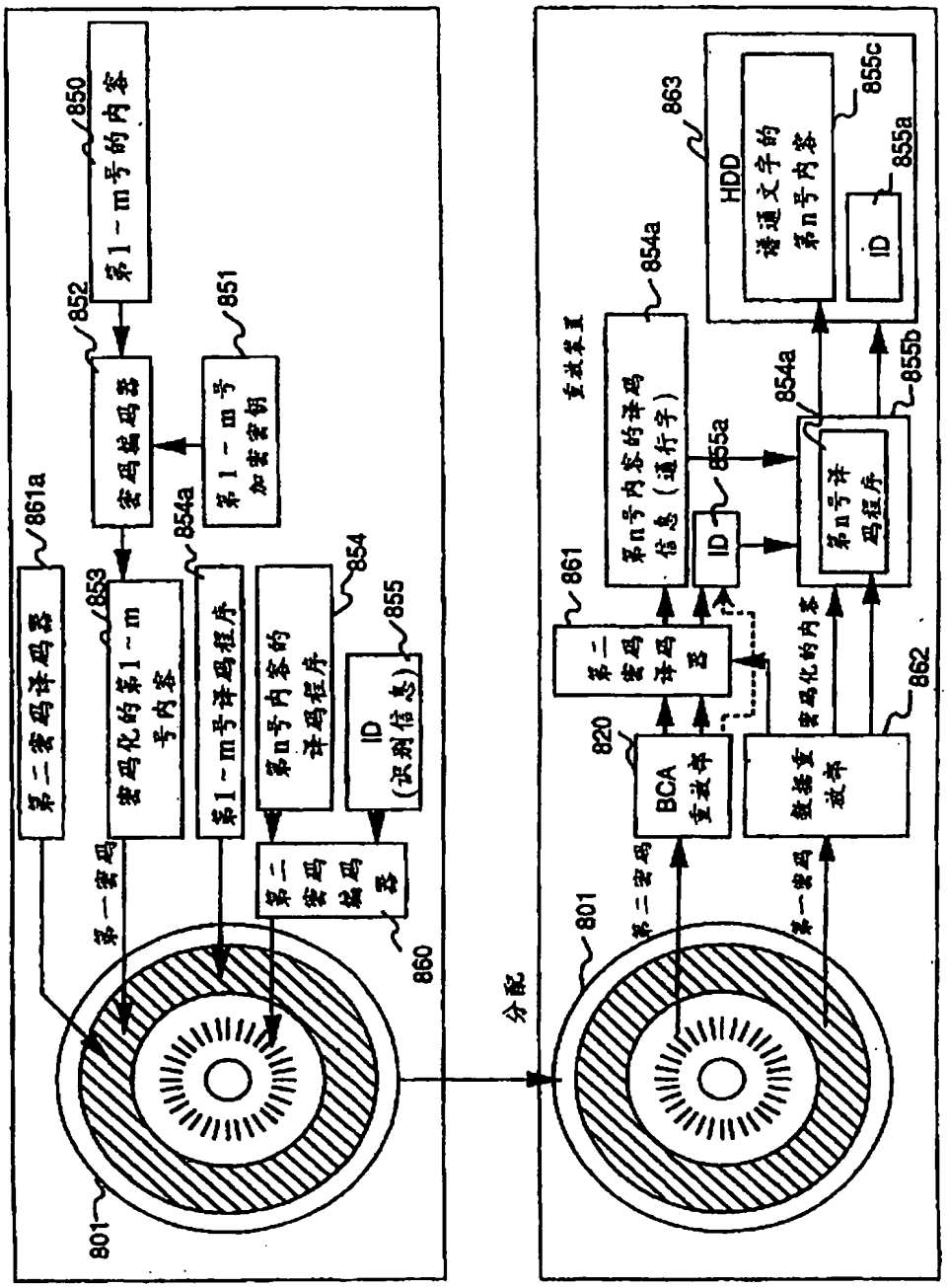

第二密码译码器
861a
密码化的第1～m号内容
853
第1～m号译码程序
854a
第n号内容的译码程序
854
ID（识别信息）
855
第二密码编码器
860
第一密码
801
密码编码器
852
第1～m号的内容
850
第1～m号加密密钥
851
分配
第二密码
第一密码
BCA重放单元
820
数据重放单元
862
第二密码译码器
861
第n号内容的译码信息（通行字）
854a
ID
855a
第n号译码程序
854a
855b
HDD
普通文字的第n号内容
855c
ID
855a
863

图 10

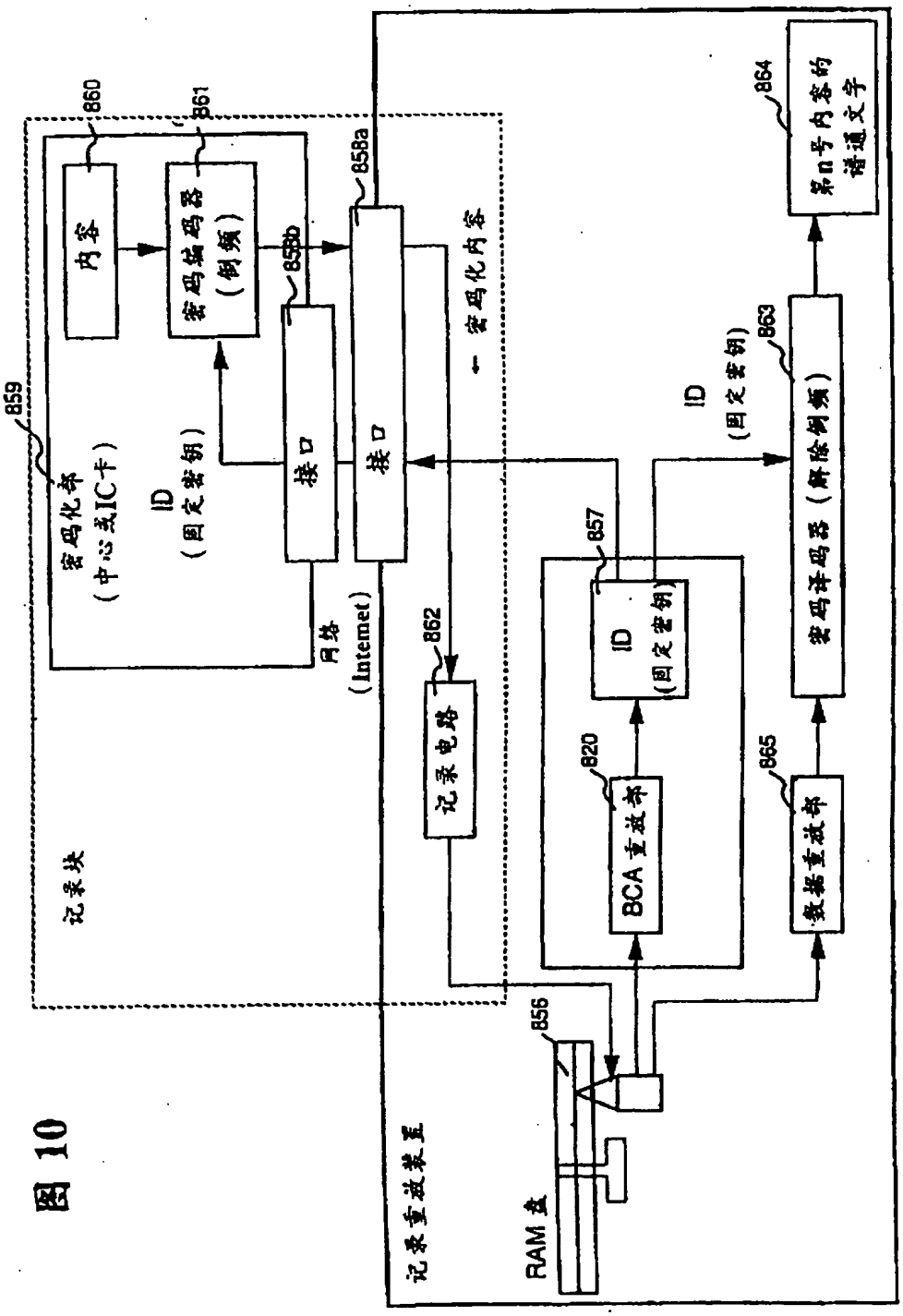

记录块
859
密码化单元
(中心或IC卡)
ID
(固定密钥)
860
内容
861
密码编码器
(例频)
858b
接口
858a
接口
网络
(Internet)
密码化内容
862
记录电路
记录重放装置
RAM 盘
856
857
ID
(固定密钥)
820
BCA 重放部
ID
(固定密钥)
863
密码译码器 (解除例频)
865
数据重放部
864
第n号内容的
播通文字

图 11

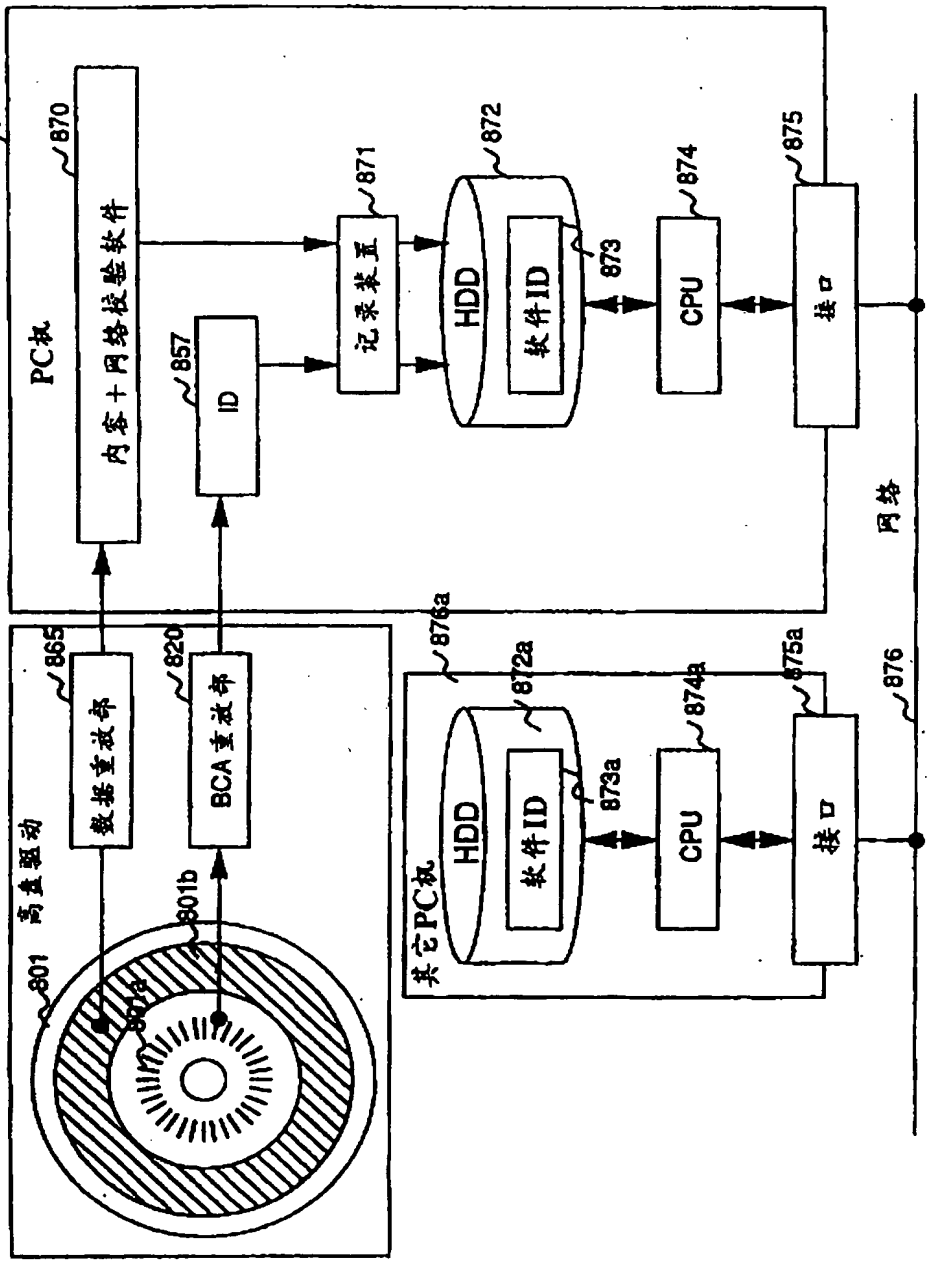

876
PC机
870
内容+网络校验软件
871
记录装置
872
HDD
软件ID
873
CPU
874
接口
875
857
ID
网络
876a
其它PC机
872a
HDD
软件ID
873a
CPU
874a
接口
875a
876
高盘驱动
801
801a
801b
865
数据重放部
820
BCA重放部

图 12

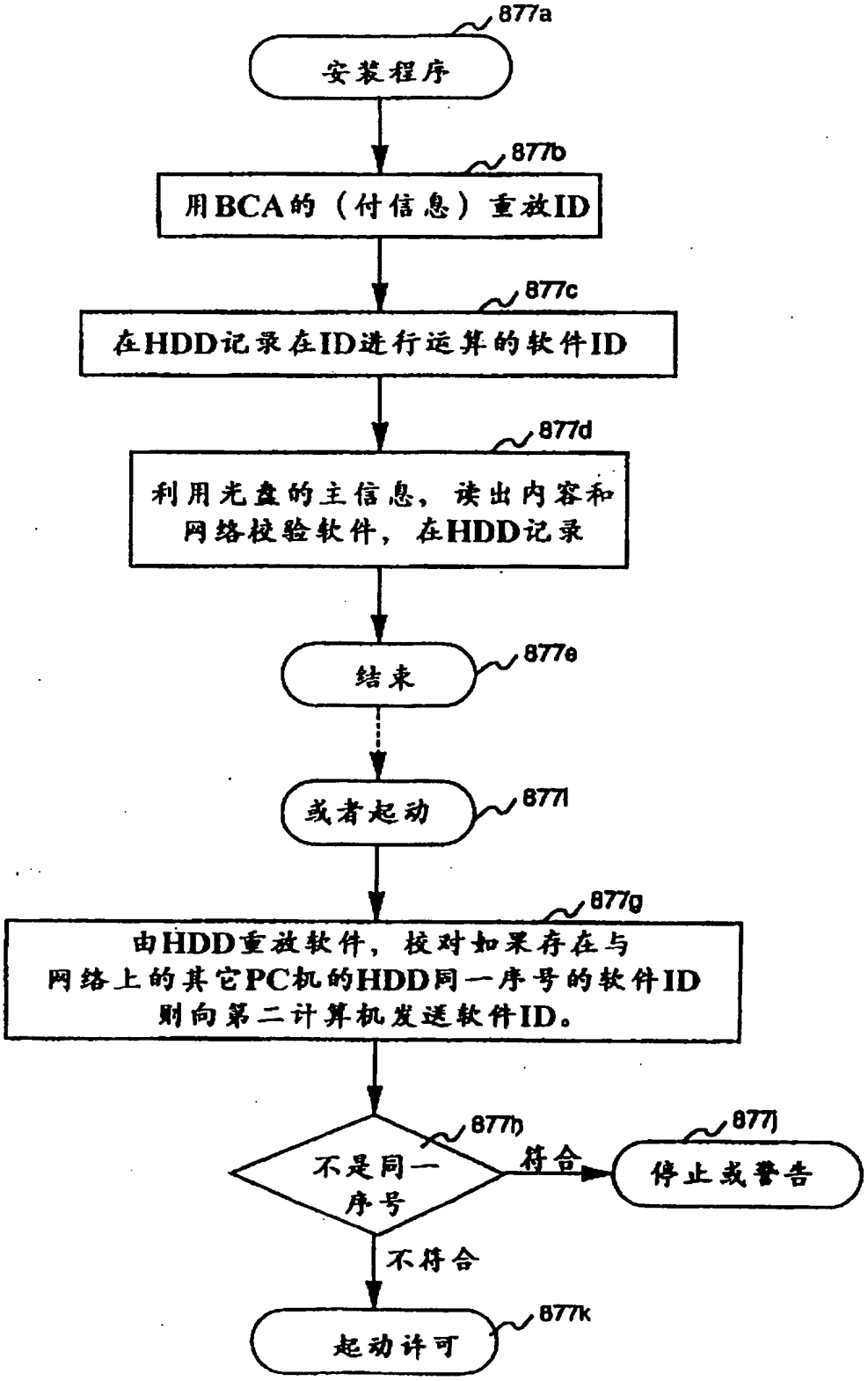

877a
安装程序
877b
用BCA的（付信息）重放ID
877c
在HDD记录在ID进行运算的软件ID
877d
利用光盘的主信息，读出内容和
网络校验软件，在HDD记录
877e
结束
877l
或者起动
877g
由HDD重放软件，校对如果存在与
网络上的其它PC机的HDD同一序号的软件ID
则向第二计算机发送软件ID。
877h
不是同一
序号
符合
877j
停止或警告
不符合
877k
起动许可

图 13

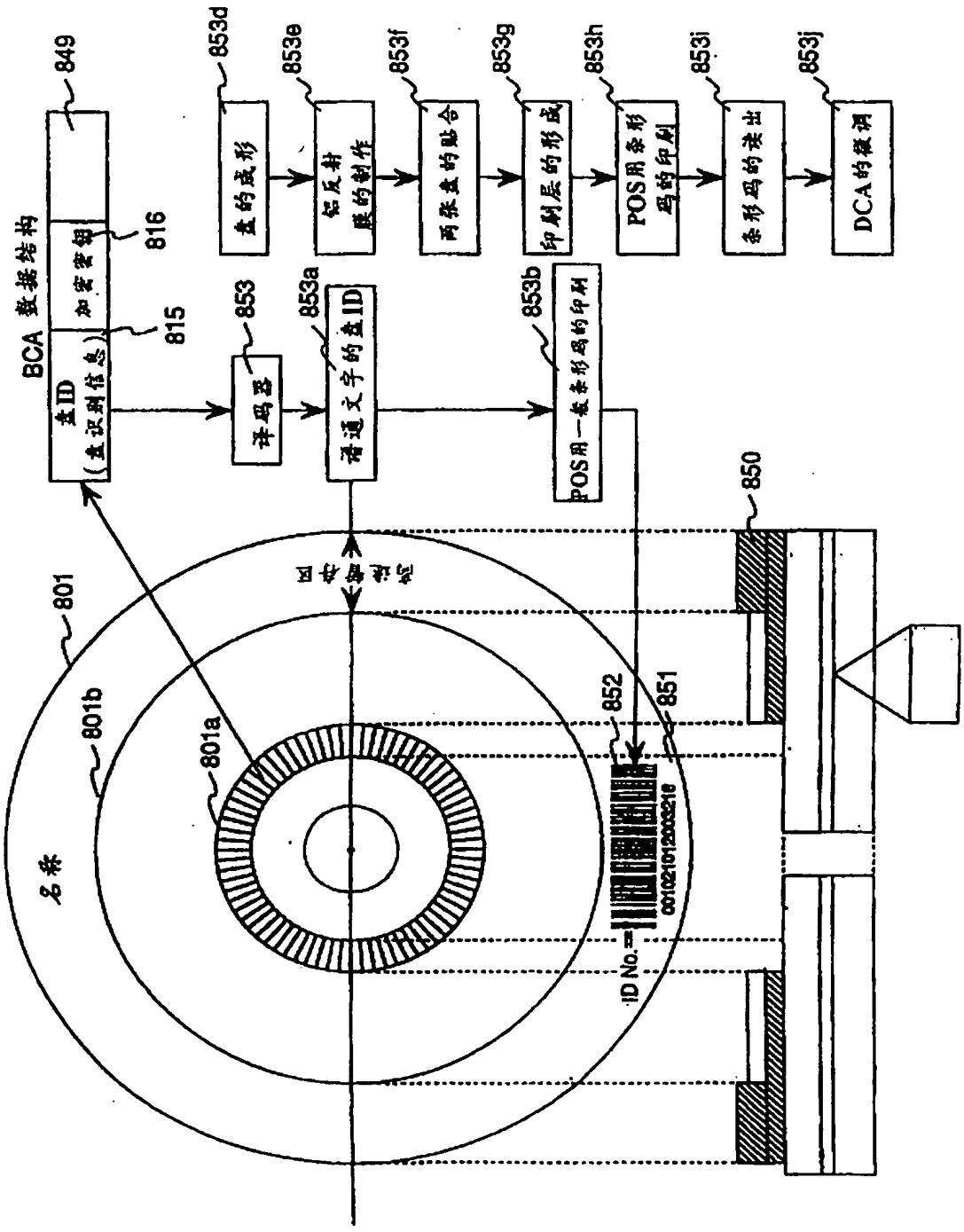

BCA 数据结构
盘ID
(盘识别信息)
加密密钥
849
816
815
853
母模器
853a
普通文字的盘ID
853b
POS用一盘母模的印刷
853d
盘的成形
853e
铝反射膜的制作
853f
两张盘的贴合
853g
印刷层的形成
853h
POS用盘形母模的印刷
853i
盘形母的读出
853j
DCA的检测
850
801
801b
801a
名称
852
851
ID No.=

图 14

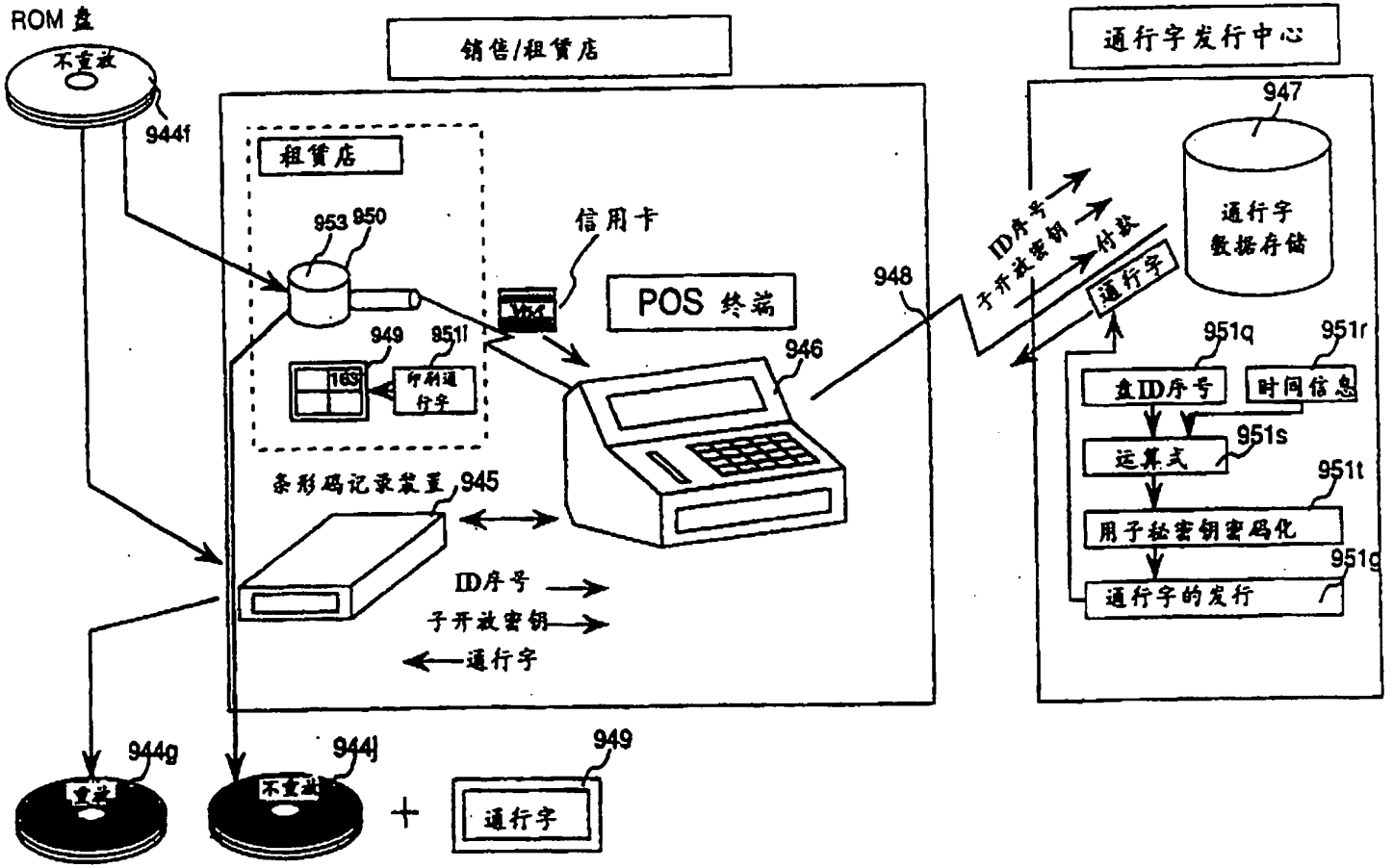

ROM 盘
不重放
9441
销售/租赁店
租赁店
953
950
信用卡
POS 终端
949
951l
印刷通行字
946
948
条形码记录装置
945
ID序号
子开放密钥
通行字
通行字发行中心
947
通行字数据存储
ID序号
子开放密钥
付款
通行字
951q
951r
盘ID序号
时间信息
951s
运算式
951t
用子秘密钥密码化
951u
通行字的发行
944g
944j
949
不重放
通行字

图 15

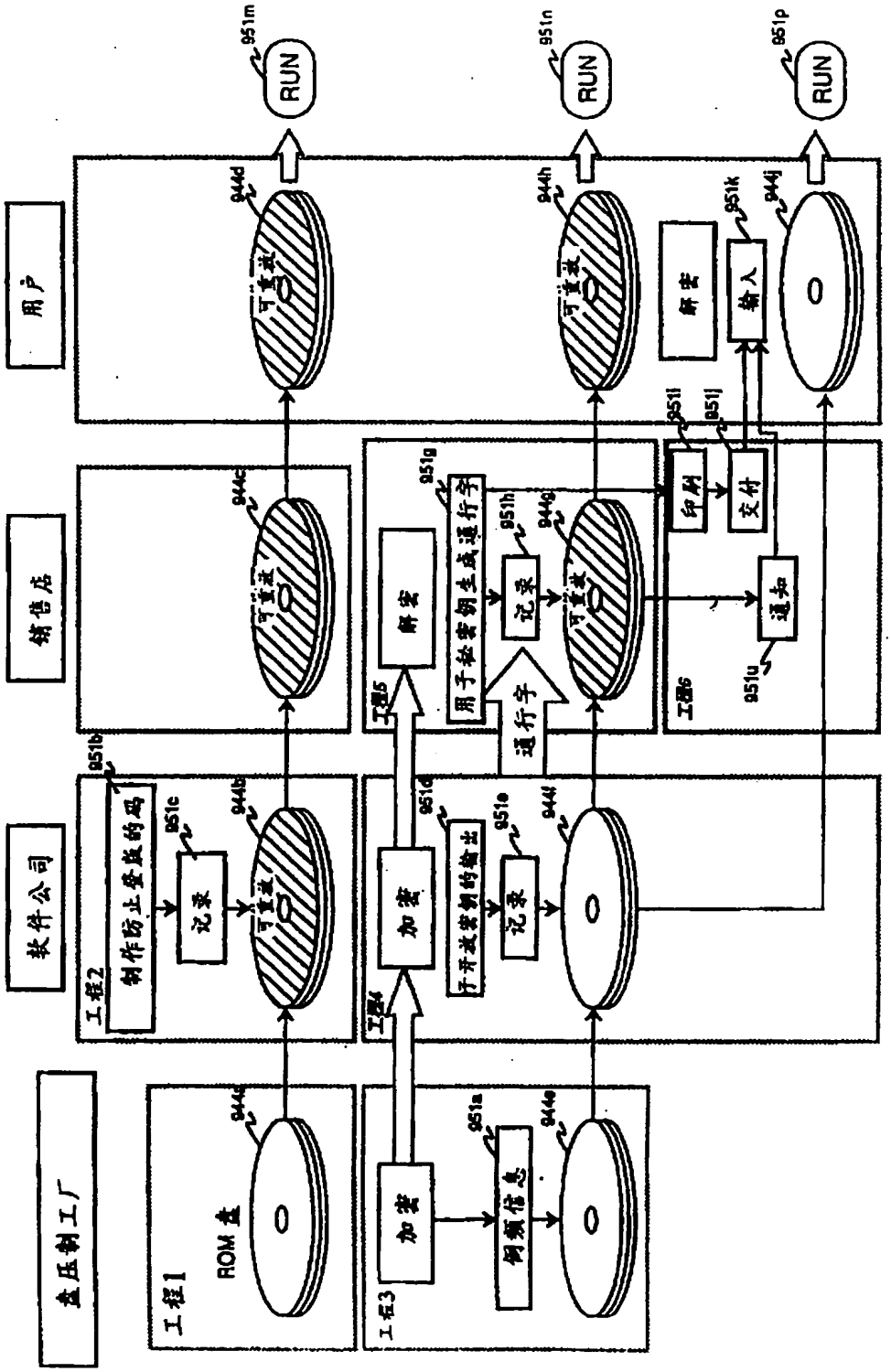

盘压制工厂
软件公司
销售店
用户
工程1
ROM 盘
工程2
制作防止坚盘的码
记录
工程3
加密
例题信息
工程4
加密
计算机密钥的输出
记录
工程5
解密
用于秘密钥生成通行字
记录
通行字
工程6
印刷
交付
通知
解密
输入
RUN
RUN
RUN

图 16

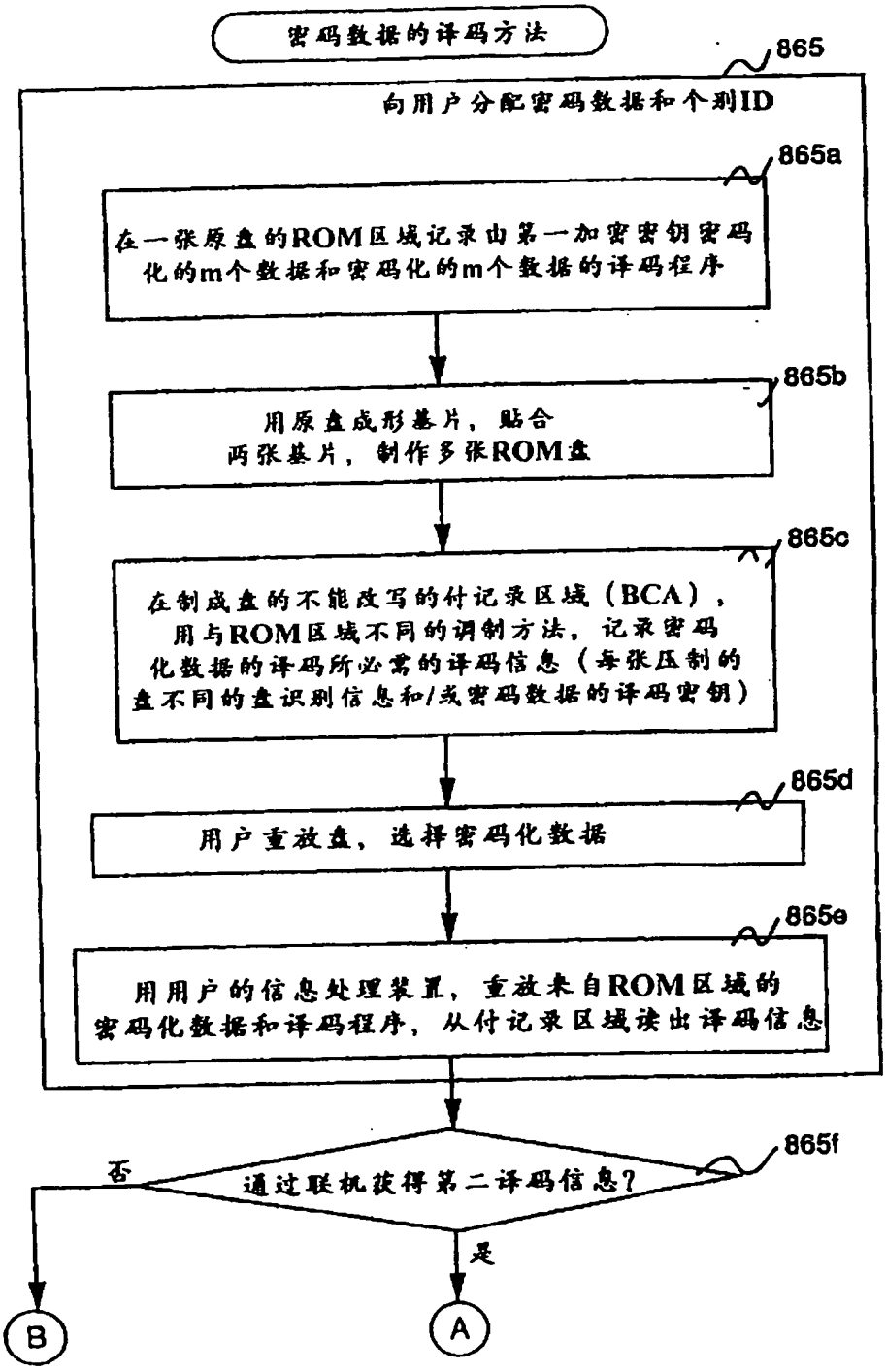

密码数据的译码方法
865
向用户分配密码数据和个别ID
865a
在一张原盘的ROM区域记录由第一加密密钥密码化的m个数据和密码化的m个数据的译码程序
865b
用原盘成形基片，贴合两张基片，制作多张ROM盘
865c
在制成盘的不能改写的付记录区域（BCA），用与ROM区域不同的调制方法，记录密码化数据的译码所必需的译码信息（每张压制的盘不同的盘识别信息和/或密码数据的译码密钥）
865d
用户重放盘，选择密码化数据
865e
用用户的信息处理装置，重放来自ROM区域的密码化数据和译码程序，从付记录区域读出译码信息
865f
通过联机获得第二译码信息？
否
是
B
A

图 17

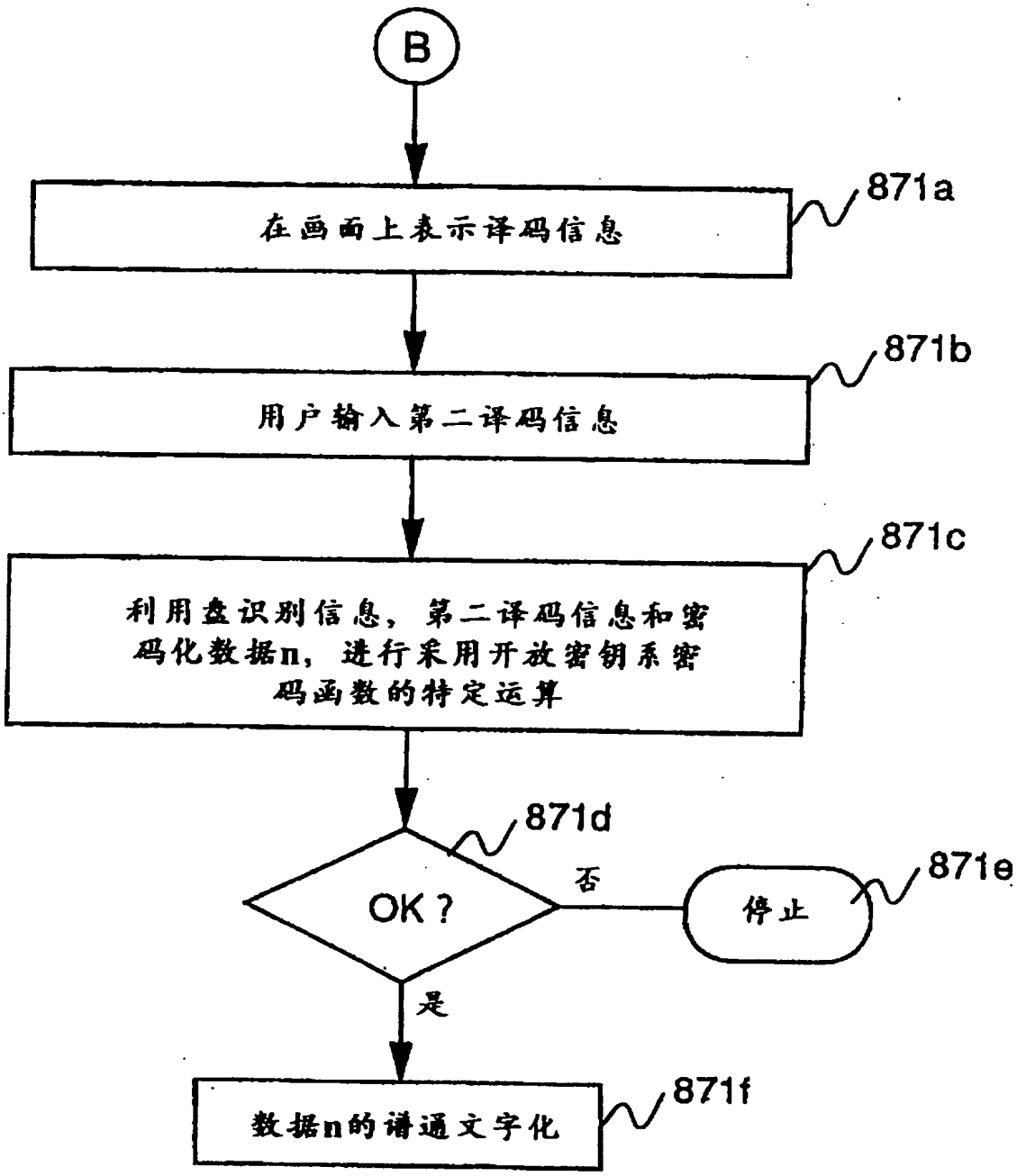

B
在画面上表示译码信息
871a
用户输入第二译码信息
871b
利用盘识别信息，第二译码信息和密码化数据n，进行采用开放密钥系密码函数的特定运算
871c
871d
OK？
否
停止
871e
是
数据n的谱通文字化
871f

图 18

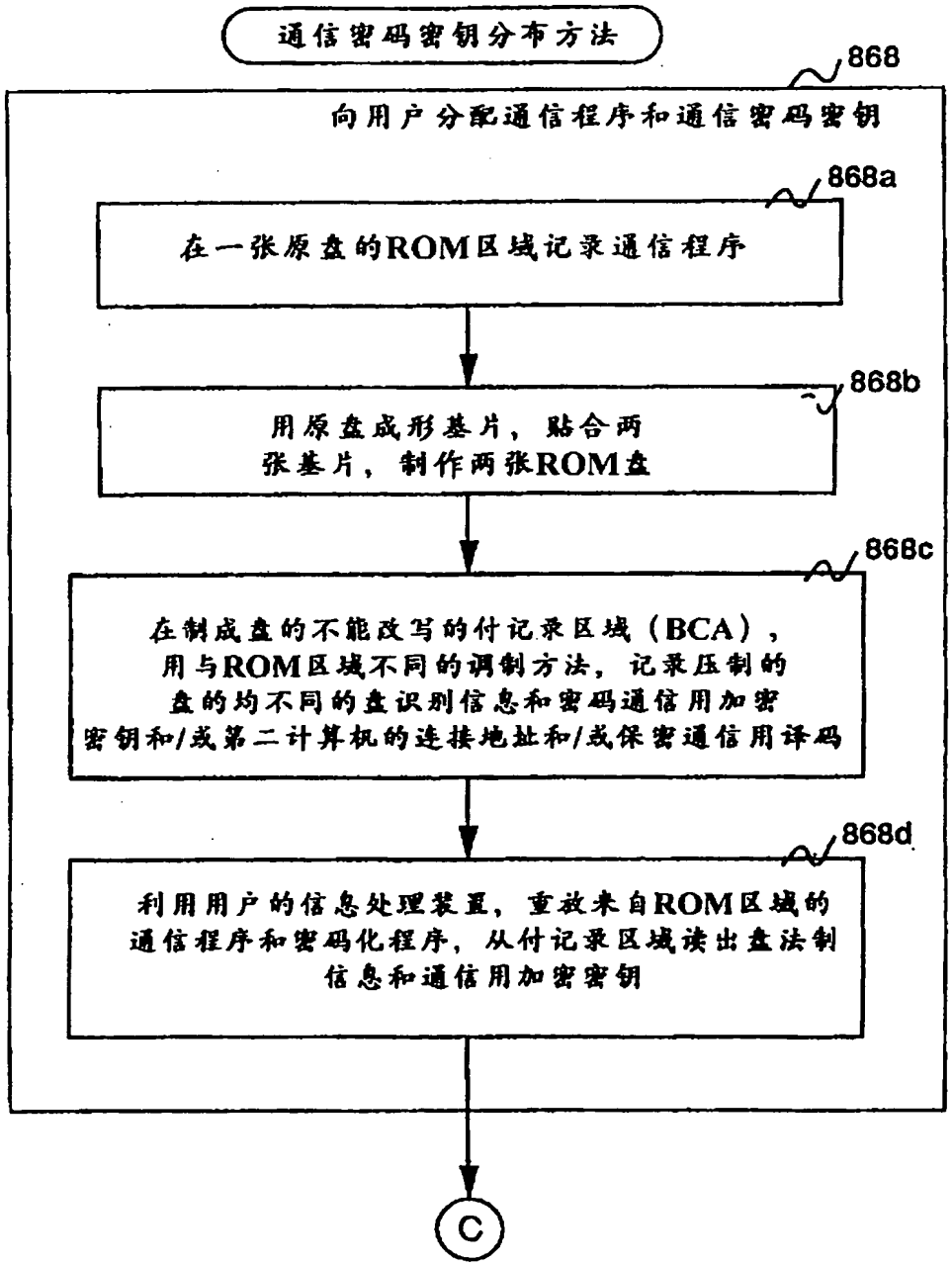

通信密码密钥分布方法
868
向用户分配通信程序和通信密码密钥
868a
在一张原盘的ROM区域记录通信程序
868b
用原盘成形基片，贴合两张基片，制作两张ROM盘
868c
在制成盘的不能改写的付记录区域（BCA），用与ROM区域不同的调制方法，记录压制的盘的均不同的盘识别信息和密码通信用加密密钥和/或第二计算机的连接地址和/或保密通信用译码
868d
利用用户的信息处理装置，重放来自ROM区域的通信程序和密码化程序，从付记录区域读出盘法制信息和通信用加密密钥
C

图 19

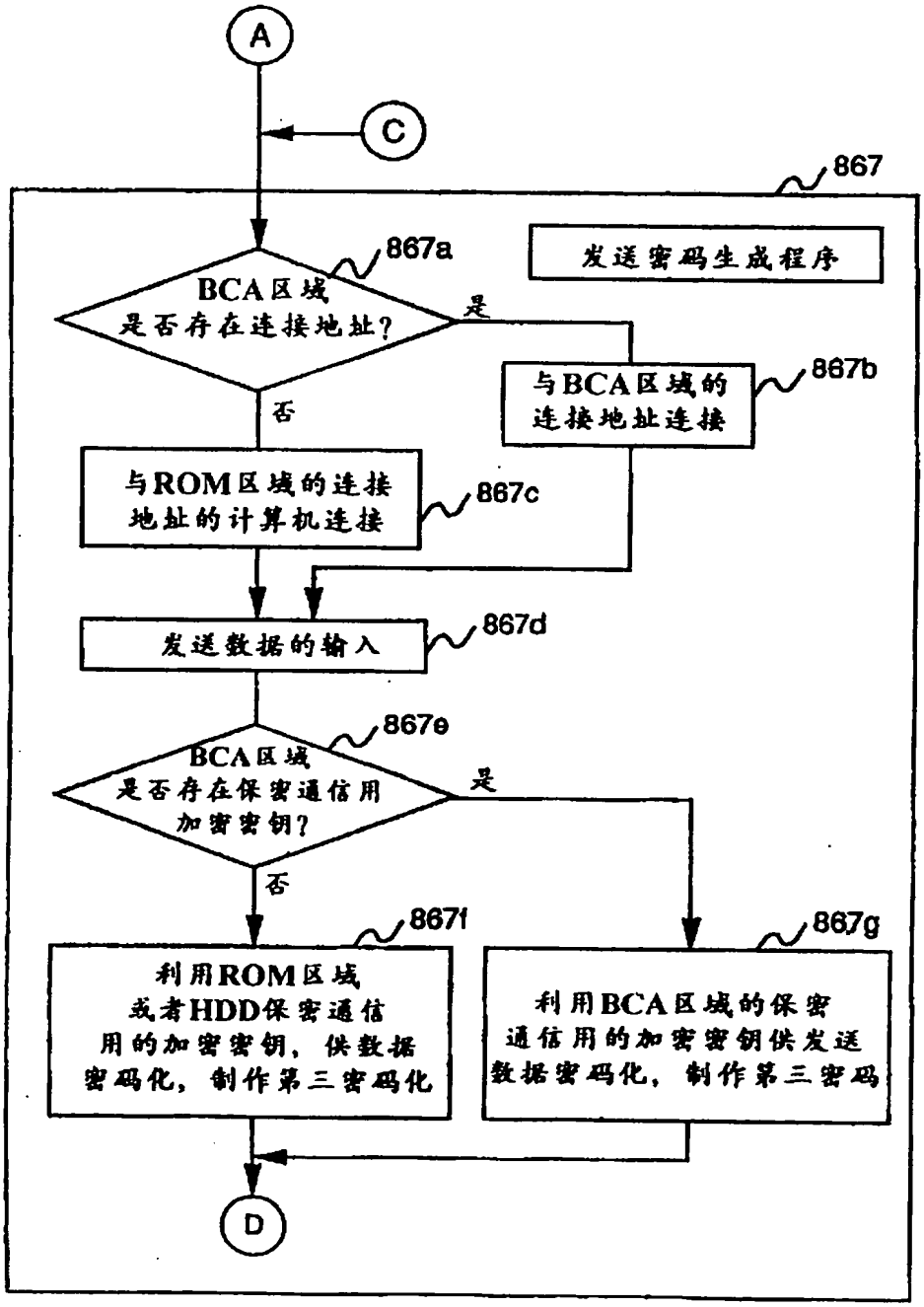

A
C
867
867a
BCA区域
是否存在连接地址?
是
否
发送密码生成程序
867b
与BCA区域的
连接地址连接
与ROM区域的连接
地址的计算机连接
867c
发送数据的输入
867d
867e
BCA区域
是否存在保密通信用
加密密钥?
是
否
867f
利用ROM区域
或者HDD保密通信
用的加密密钥，供数据
密码化，制作第三密码化
867g
利用BCA区域的保密
通信用的加密密钥供发送
数据密码化，制作第三密码
D

图 20

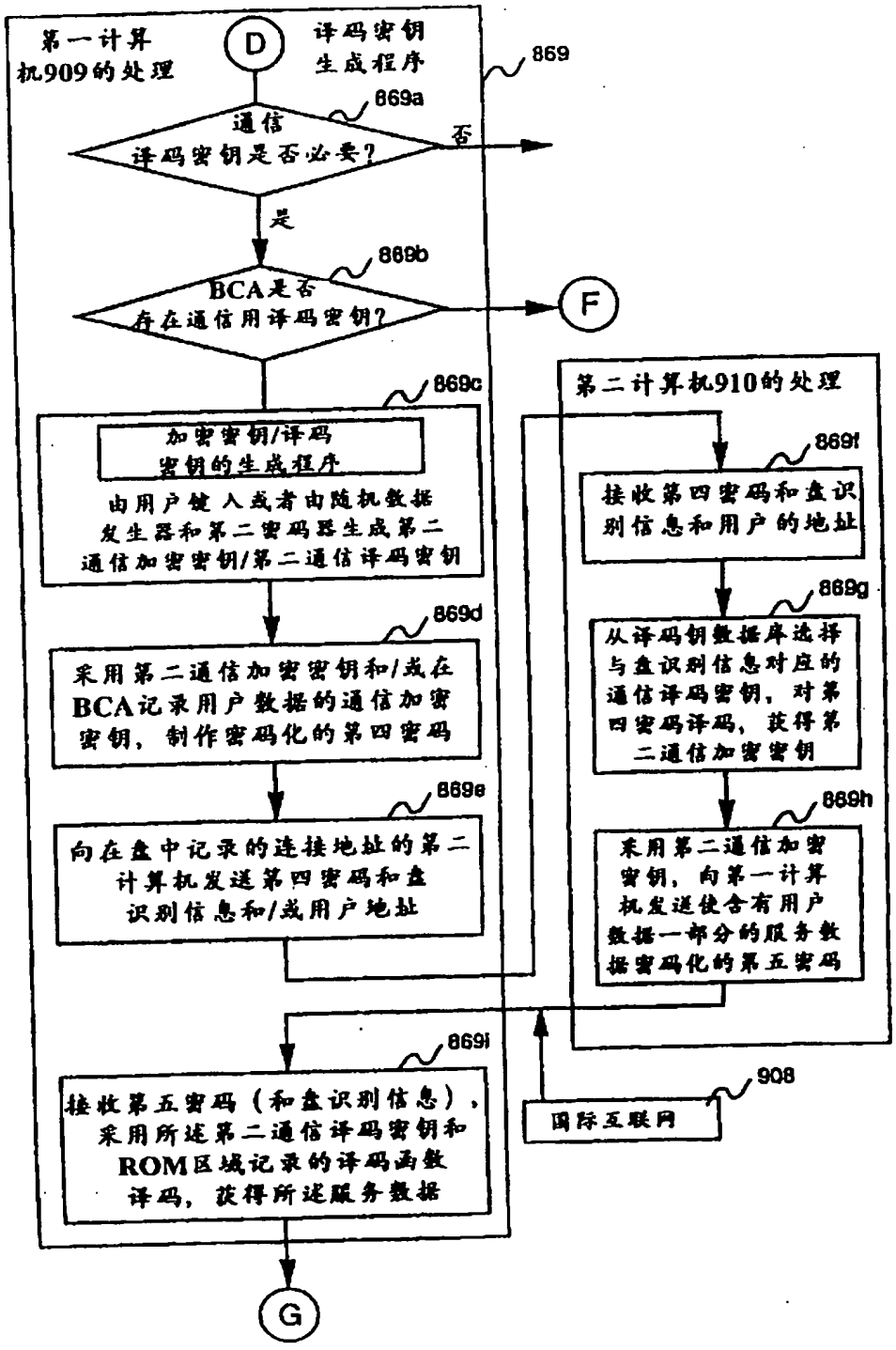

第一计算机909的处理
D
译码密钥生成程序
869
869a
通信译码密钥是否必要?
否
是
869b
BCA是否存在通信用译码密钥?
F
869c
加密密钥/译码密钥的生成程序
由用户键入或者由随机数发生器和第二密码器生成第二通信加密密钥/第二通信译码密钥
869d
采用第二通信加密密钥和/或在BCA记录用户数据的通信加密密钥，制作密码化的第四密码
869e
向在盘中记录的连接地址的第二计算机发送第四密码和盘识别信息和/或用户地址
869i
接收第五密码（和盘识别信息），采用所述第二通信译码密钥和ROM区域记录的译码函数译码，获得所述服务数据
G
第二计算机910的处理
869f
接收第四密码和盘识别信息和用户的地址
869g
从译码钥数据库选择与盘识别信息对应的通信译码密钥，对第四密码译码，获得第二通信加密密钥
869h
采用第二通信加密密钥，向第一计算机发送使含有用户数据一部分的服务数据密码化的第五密码
908
国际互联网

图 21

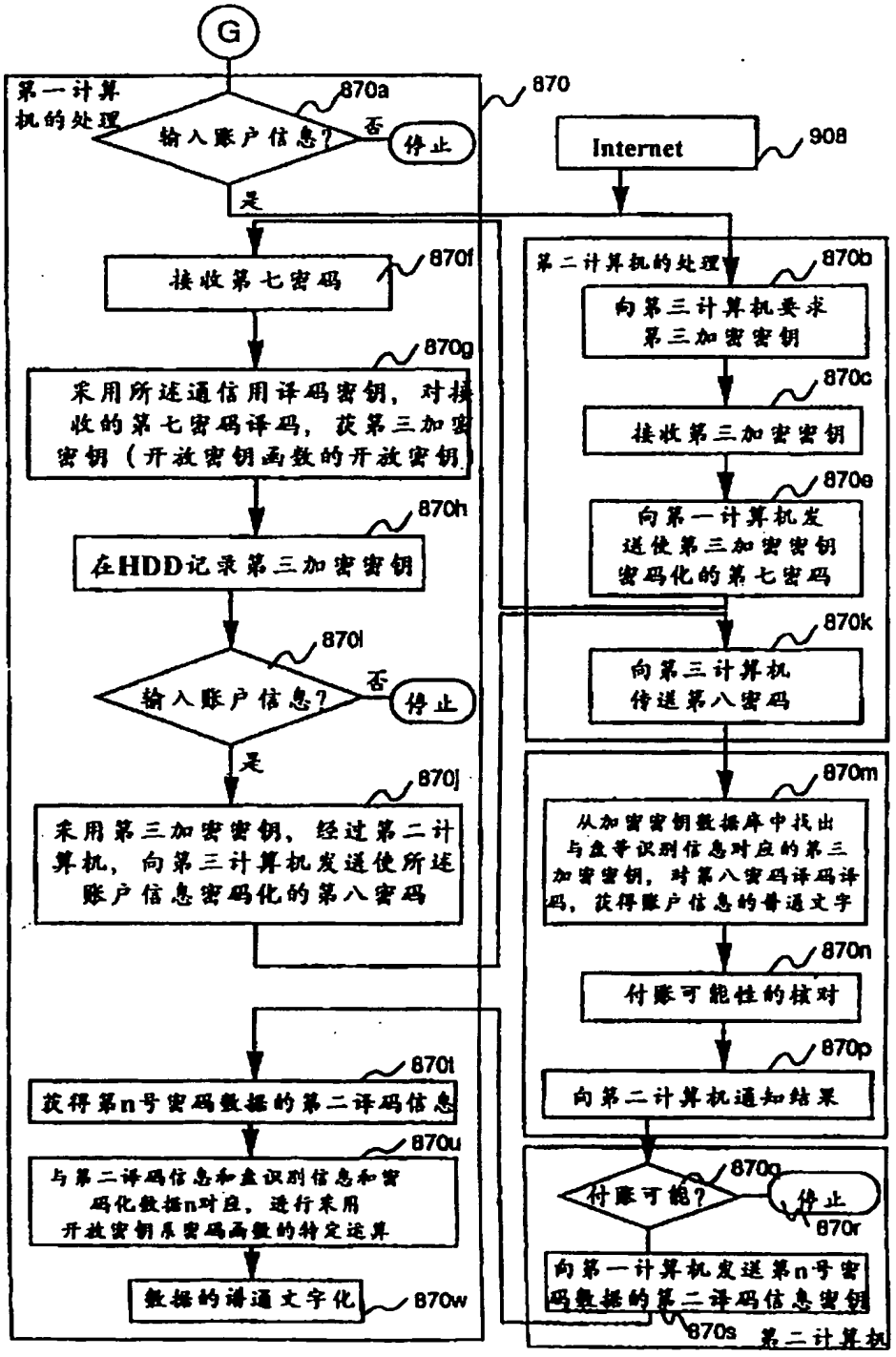

G
第一计算机的处理
870a
输入账户信息?
否
停止
是
870
Internet
908
接收第七密码
870f
870g
采用所述通信用译码密钥，对接收的第七密码译码，获第三加密密钥（开放密钥函数的开放密钥）
870h
在HDD记录第三加密密钥
870i
输入账户信息?
否
停止
是
870j
采用第三加密密钥，经过第二计算机，向第三计算机发送使所述账户信息密码化的第八密码
870t
获得第n号密码数据的第二译码信息
870u
与第二译码信息和盘识别信息和密码化数据n对应，进行采用开放密钥系密码函数的特定运算
数据的普通文字化
870w
第二计算机的处理
870b
向第三计算机要求第三加密密钥
870c
接收第三加密密钥
870e
向第一计算机发送使第三加密密钥密码化的第七密码
870k
向第三计算机传送第八密码
870m
从加密密钥数据库中找出与盘号识别信息对应的第三加密密钥，对第八密码译码译码，获得账户信息的普通文字
870n
付账可能性的核对
870p
向第二计算机通知结果
870q
付账可能?
停止
870r
向第一计算机发送第n号密码数据的第二译码信息密钥
870s
第二计算机

图 22

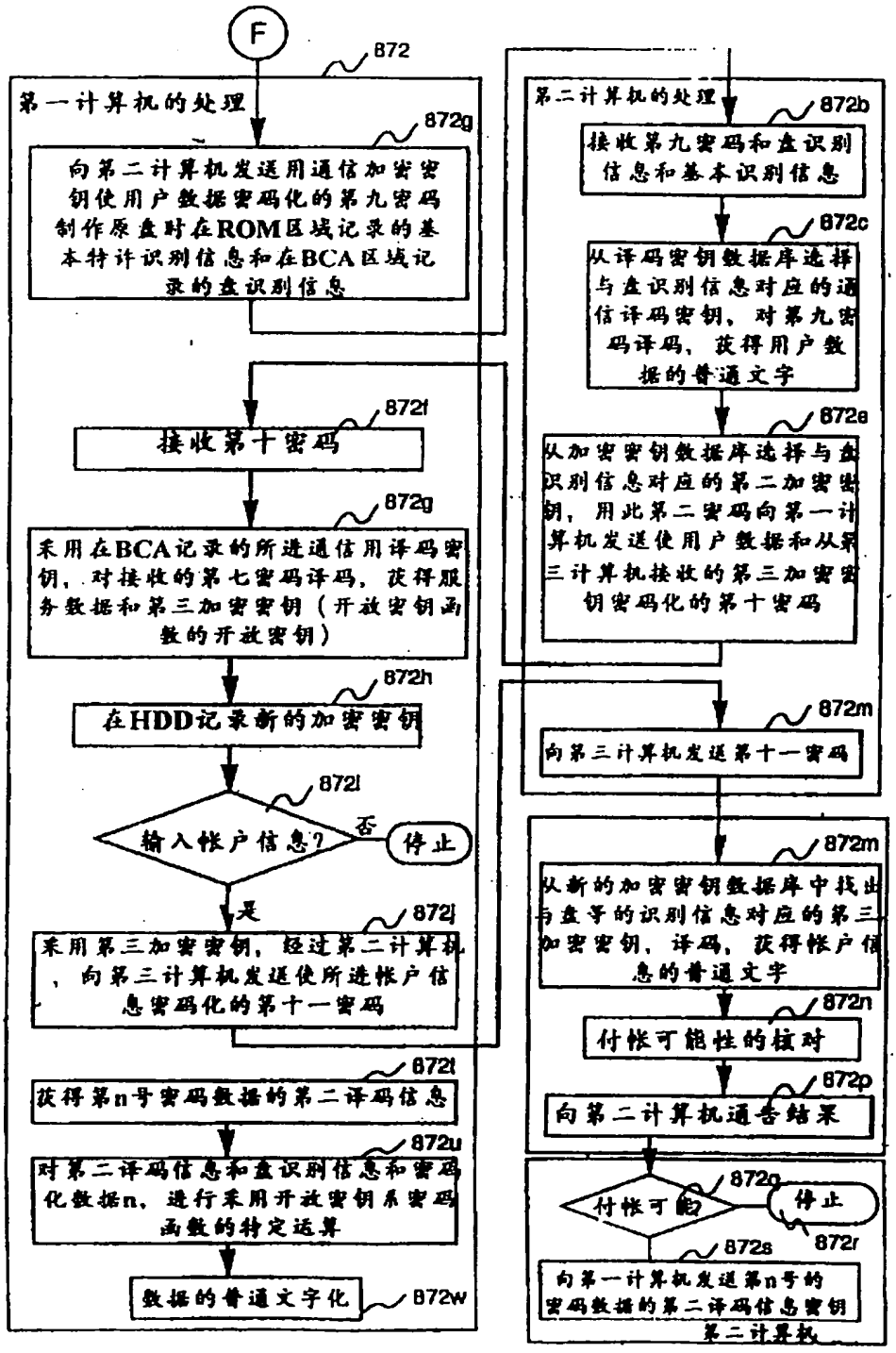

F
872
第一计算机的处理
872g
向第二计算机发送用通信加密密钥使用户数据密码化的第九密码制作原盘时在ROM区域记录的基本特许识别信息和在BCA区域记录的盘识别信息
872t
接收第十密码
872g
采用在BCA记录的所述通信用译码密钥，对接收的第七密码译码，获得服务数据和第三加密密钥（开放密钥函数的开放密钥）
872h
在HDD记录新的加密密钥
872i
输入帐户信息?
否
停止
是
872j
采用第三加密密钥，经过第二计算机，向第三计算机发送使所述帐户信息密码化的第十一密码
872t
获得第n号密码数据的第二译码信息
872u
对第二译码信息和盘识别信息和密码化数据n，进行采用开放密钥系密码函数的特定运算
数据的普通文字化
872w
第二计算机的处理
872b
接收第九密码和盘识别信息和基本识别信息
872c
从译码密钥数据库选择与盘识别信息对应的通信译码密钥，对第九密码译码，获得用户数据的普通文字
872e
从加密密钥数据库选择与盘识别信息对应的第二加密密钥，用此第二密码向第一计算机发送使用户数据和从第三计算机接收的第三加密密钥密码化的第十密码
872m
向第三计算机发送第十一密码
872m
从新的加密密钥数据库中找出与盘号的识别信息对应的第三加密密钥，译码，获得帐户信息的普通文字
872n
付帐可能性的核对
872p
向第二计算机通告结果
872q
付帐可能?
停止
872r
872s
向第一计算机发送第n号的密码数据的第二译码信息密钥
第二计算机

图 23

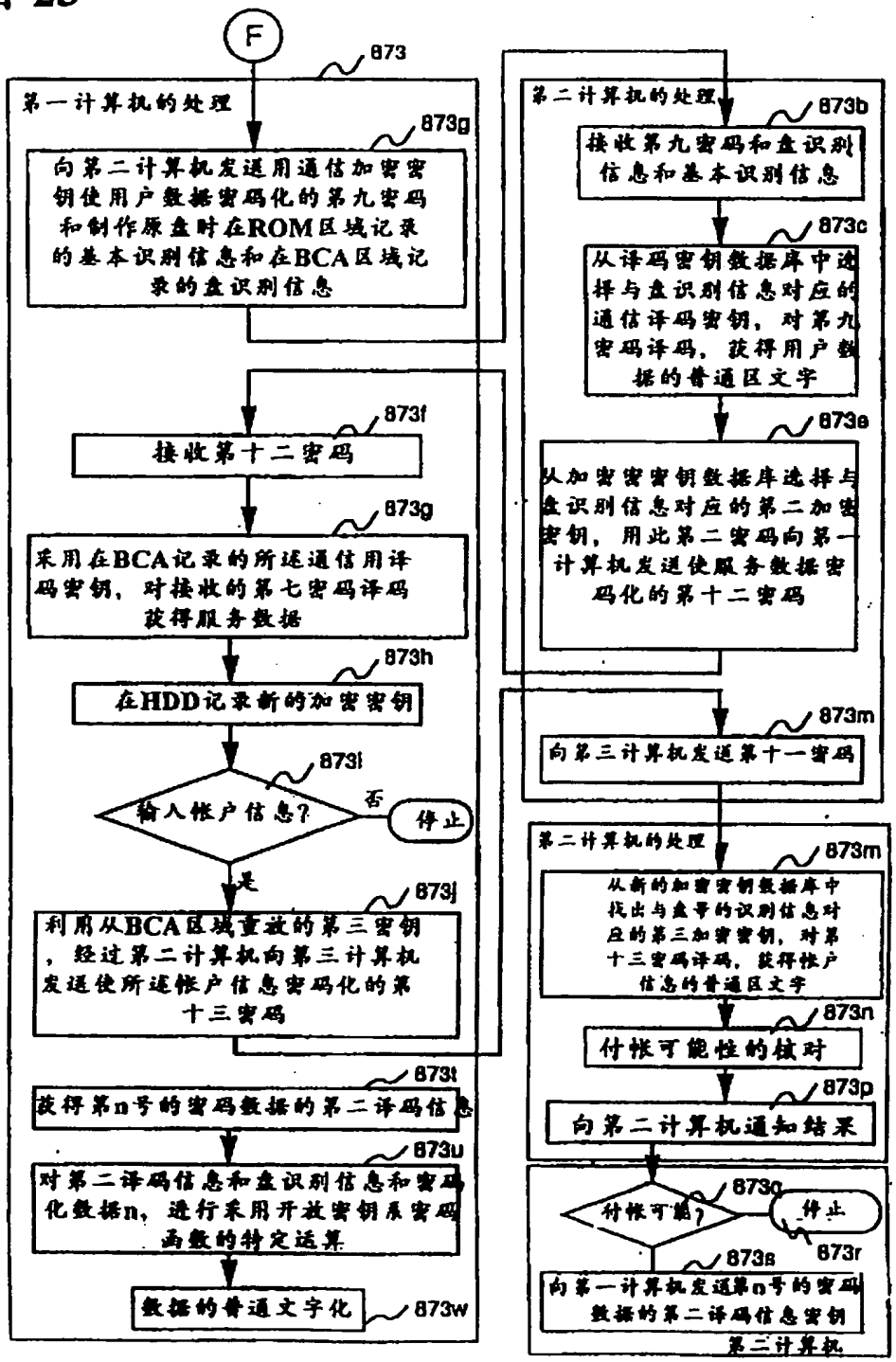
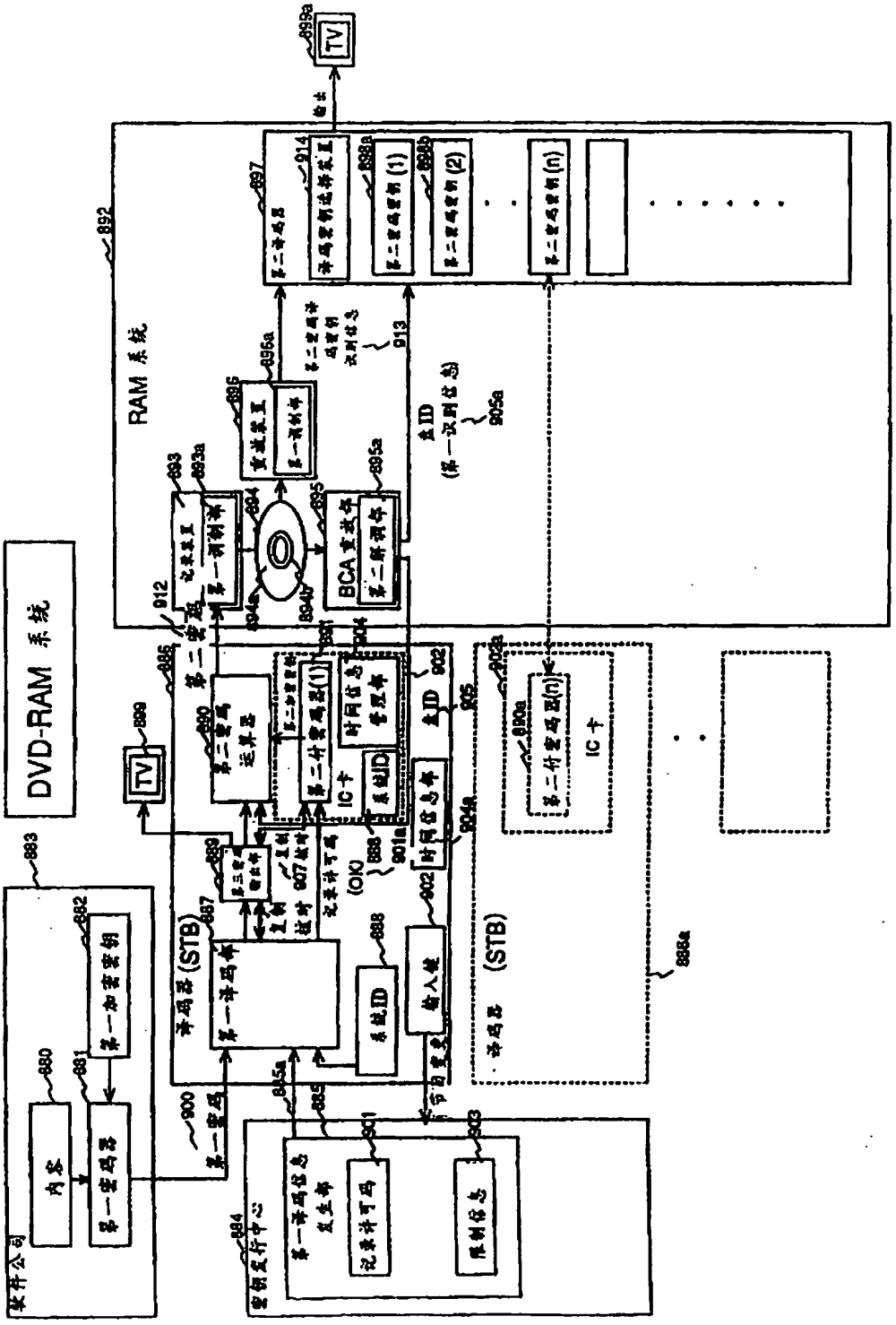

F
873
第一计算机的处理
873g
向第二计算机发送用通信加密密钥使用户数据密码化的第九密码和制作原盘时在ROM区域记录的基本识别信息和在BCA区域记录的盘识别信息
873f
接收第十二密码
873g
采用在BCA记录的所述通信用译码密钥，对接收的第七密码译码获得服务数据
873h
在HDD记录新的加密密钥
873i
输入帐户信息?
否
停止
是
873j
利用从BCA区域重放的第三密钥，经过第二计算机向第三计算机发送使所述帐户信息密码化的第十三密码
873t
获得第n号的密码数据的第二译码信息
873u
对第二译码信息和盘识别信息和密码化数据n，进行采用开放密钥系密码函数的特定运算
数据的普通文字化
873w
第二计算机的处理
873b
接收第九密码和盘识别信息和基本识别信息
873c
从译码密钥数据库中选择与盘识别信息对应的通信译码密钥，对第九密码译码，获得用户数据的普通区文字
873e
从加密密密钥数据库选择与盘识别信息对应的第二加密密钥，用此第二密码向第一计算机发送使服务数据密码化的第十二密码
873m
向第三计算机发送第十一密码
第二计算机的处理
873m
从新的加密密钥数据库中找出与盘号的识别信息对应的第三加密密钥，对第十三密码译码，获得帐户信息的普通区文字
873n
付帐可能性的核对
873p
向第二计算机通知结果
873q
付帐可能?
停止
873r
873s
向第一计算机发送第n号的密码数据的第二译码信息密钥
第三计算机

图 24



附图标号一览表

801… 带 BCA 的盘
802… 固定键
803… 密码编码器
804… 记录装置
805… 内容
806… ID
807… 微调装置
808a… 成形机
808b… 反射膜形成机
808c… 贴合机
809… 制成盘
809a… 单面盘
809b… 单面盘
811… 压制工厂
813… 固定键
814… BCA 区域
815… 盘 ID
816… 第 1 密码键（秘密键）
817… 第 2 密码键（秘密键）
818… 连接地址
819… 重放装置
820… BCA 重放部
821… 通行字发行中心
822… 通信部
823… 网络
824… 密钥 DB
825… 第 1 解码密钥
826… 内容编码

827… 第 1 密码译码器
828… 收费中心
829… 第 2 解码密钥
830… 收费信息
831… 第 2 密码编码器
832… 第 2 密码译码器
833… 时间信息
834… 通行字生成部
835… 通行字
836… PC 机
837… 第 3 解码密钥
838… 共用密钥
839… 第 3 密钥
840… 第 3 密码编码器
841… 第 3 密码译码器
842… 主密码编码器
843… 主密码解码器
844… 主解码密钥
845… 第 1 密码译码器
846… 密码编码器
847… 密码译码器
849… BCA 数据
850… 写入层
851… 文字
852… 一般条形码
853… 解码器
860… 第 2 密码编码器
861… 第 2 密码译码器
862… 数据重放部

863… ROM 区域
864… 补记区域
865… 解码流程图
890… 第 2 密码运算器
894a… 第 1 记录区域
908… 因特网
909… 第 1 计算机
910… 第 2 计算机
911… 第 3 计算机
912… 第 2 密码
913… 解码密钥识别信息
914… 解码密钥选择装置
915… 第 1 削波电平
916… 第 2 削波电平
917… PE － RZ 调制器
918… 透明基板
919… 第 1 记录区域
920… 第 2 记录区域
921… 盘 ID
922… BCA 标志
923… CPU
924… 控制数据
925… EFM 解调
926… 8 － 15 调制解调
927… 8 － 16 调制解调
928… 第 1 解调部
930… 第 2 解调部
931… 连接地址

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- [x] BLACK BORDERS
- [ ] IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- [x] FADED TEXT OR DRAWING
- [x] BLURRED OR ILLEGIBLE TEXT OR DRAWING
- [ ] SKEWED/SLANTED IMAGES
- [ ] COLOR OR BLACK AND WHITE PHOTOGRAPHS
- [ ] GRAY SCALE DOCUMENTS
- [ ] LINES OR MARKS ON ORIGINAL DOCUMENT
- [ ] REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- [ ] OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.